AMERICAN Journal of Engineering,
Mechanics and Architecture
Volume 2, Issue 4, 2024 ISSN (E): 2993-2637

Basic Characteristics of Using Identity Management Technology

Rustam Qodirov
Lecturer of the department, Informatics and management National institute of fine art and design named after K.Behzod, Uzbekistan, Tashkent

Abstract: This article discusses the basic features of using Identity Management technology. Accordingly, to manage personal data in IT, large companies will be forced to implement specialized IDM-class systems to manage information about users of their corporate systems. If earlier there was a certain shortage of qualified personnel in this area, now this shortage will take on catastrophic proportions, since thunder has struck and the peasant must begin to be baptized.

Keywords: online systems, identity management, IAM, IdM.

The shortage of personnel in this specialized area is due to the fact that an IDM specialist must have several IT skills at once - he must be well versed in the design of various information security systems, have practical experience in system administration, be a good programmer for writing adapters and data processing scripts, be able to describe and set up business processes. And at the same time, he should not be infuriated by the huge amount of routine work on reconciling personal data. I can say with almost 100% certainty that such people do not exist in nature.

This fact is associated with the eternal headache of HR employees, who generally have a vague idea of our specifics, and now they have to deal with such an explosive mixture of incompatible skills.

The only way out of the situation is to divide the work into at least two people. One can program connectors to security systems, configure internal workflows, write scripts and handle deployment. The second should work with user data, describe business processes, document and promote the idea of IDM to the IT masses.

Identity management (ID management) - or identity and access management (IAM) - are the organizational and technical processes for first registering and authorizing access rights at the configuration stage, and then at the operational stage to identify, authenticate and control individuals or groups of people have access to applications, systems or networks based on previously authorized access rights. Identity management (IdM) is the task of managing information about users on computers. Such information includes information that identifies the user and information that describes the data and actions that they are authorized to access and/or perform. It also includes managing descriptive information about the user, as well as how and who can access and change this information. In addition to users, managed objects typically include hardware, network resources, and even applications. The diagram below shows the relationship between the configuration and operation phases of IAM, and the difference between identity management and access management.

In the real context of developing online systems, identity management can include four main functions: Pure identity function: creating, managing and deleting identities without regard to access or rights; User access (login) function: For example: smart card and associated data used by a client to log into a service or services (traditional view); Service Function: A system that provides personalized, role-based, online, on-demand, and presence-based multimedia (content) services to users and their devices. Identity Federation: A system that relies on federated identity to authenticate a user without knowing their password.

A general identity model can be constructed from a small set of axioms, such as that all identities in a given namespace are unique, or that such identities have a specific relationship to corresponding entities in the real world. Such an axiomatic model expresses “pure identity” in the sense that the model is not limited to a specific application context. In general, an object (real or virtual) can have multiple identifiers, and each identifier can include multiple attributes, some of which are unique in a given namespace. The diagram below shows the conceptual relationships between identifiers and objects, and between identifiers and their attributes. In most theoretical and all practical models of digital identity, a given identity object consists of a finite set of properties (attribute values).

These properties record information about an object, either for purposes external to the model or for manipulation of the model, such as classification and extraction. The "pure identity" model does not strictly address the external semantics of these properties. The most common deviation from "pure identity" in practice occurs with properties intended to provide some aspect of identity, such as a digital signature or software token that the model can use internally to verify some aspect of identity to satisfy an external goal. Because the model internally expresses such semantics, it is not a pure model. Contrast this situation with properties that can be used externally for information security purposes such as access or rights control, but which are simply stored, maintained, and retrieved without much processing of the model. The absence of external semantics in the model qualifies it as a “pure identity” model. Identity management can thus be defined as a set of operations on a given identity model or, more generally, as a set of capabilities associated with it. In practice, identity management is often extended to express how model content should be prepared and consistent across multiple identity models.

User access allows users to assume a certain digital identity in applications, allowing access controls to be assigned and assessed against that identity. Using one identity for a given user across multiple systems simplifies tasks for administrators and users. This simplifies monitoring and auditing of access and allows organizations to minimize excessive privileges granted to a single user. User access can be tracked from start to termination of user access. When organizations deploy an identity management process or system, their motivation is typically not to manage a set of identities, but rather to grant appropriate access rights to those entities through their identities. In other words, access control is typically the motivation for identity management, and hence the two sets of processes are closely related.

Organizations continue to add services for both internal users and customers. Many such services require identity management to properly provide these services. Increasingly, identity management is being decoupled from application functionality so that a single identity can serve many or even all of an organization's activities. For internal use, identity management is evolving to control access to all digital assets, including devices, network equipment, servers, portals, content, applications and/or products. Services often require access to extensive user information, including address books, preferences, rights, and contact information. Since much of this information is subject to privacy and/or confidentiality requirements, controlling access to it is vital.

In addition to assisted or self-service creation, deletion, modification of user identities, Identity Management controls ancillary entity data for use by applications, such as contact information or location.

Authentication: Verifying who/what claims an entity is using a password, biometrics such as a fingerprint, or distinctive behavior such as a touchscreen gesture pattern.

Authorization: Management of authorization information that determines what operations an object can perform in the context of a particular application. For example, one user may be allowed to enter a sales order, and another user may be allowed to approve a credit request for that order.

Roles: Roles are groups of activities and/or other roles. Users are assigned roles, often associated with a specific job or job function. Roles are granted permissions by effectively granting permission to all users who have been granted the role. For example, the user administrator role may be authorized to reset a user's password, and the system administrator role may have the ability to assign a user to a specific server.

Delegation: Delegation allows local administrators or supervisors to make changes to the system without a global administrator or allow one user to perform actions on their behalf. For example, a user can delegate the right to manage proprietary information.

Exchange: The SAML protocol is an important means used to exchange identity information between two identity domains. OpenID Connect is another such protocol.

References:

1. Fayziyev, T., Zunnunova, U., & Zakirova, S. (2020). Academic and organizational aspects of entrepreneurship education in art universities of Uzbekistan. *Journal of critical reviews*, *7*, 19.
2. Zakirova, S. A., & Zunnunova, U. G. (2021). Classification Of Creative Industries In Uzbekistan. *Nveo-natural volatiles & essential oils journal| nveo*, 15296-15302.
3. Mukhamedov, U. S. (2021). Trends In The Emergence And Development Of Styles In Web-Design. *The American Journal of Interdisciplinary Innovations and Research*, *3*(10), 21-24.
4. Мирзаюнусова З. И. Расулова М. Х. (2011). Роль образа исторической личности в воспитании гармонично развитой личности. МОЛОДЕЖЬ И НАУКА: РЕАЛЬНОСТЬ И БУДУЩЕЕ. Материалы IV Международной научно-практической конференции, 1, 572-573.
5. Расулов, И., & Хамдамова, М. (2020). Лексико-грамматическая характеристика адъективных фразеологизмов. *Иностранная филология: язык, литература, образование*, (1 (74)), 128-132.
6. Kiramidinovna, I. D., & Diyora, A. (2023). IMPORTANCE OF FORMATION AND DEVELOPMENT OF CREATIVITY SKILLS AMONG STUDENTS IN TEACHING GENERAL TECHNICAL SUBJECTS. *INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLINARY RESEARCH ISSN: 2277-3630 Impact factor: 7.429*, *12*(03), 39-41.
7. Kiramidinovna, I. D., & Rustam, M. (2023). Talabalarni ijodiy qobiliyatlarini rivojlantirishda tizimli tahlil va qaror qabul qilish texnologiyalari: talabalarni ijodiy qobiliyatlarini rivojlantirishda tizimli tahlil va qaror qabul qilish texnologiyalari.
8. Kiramidinovna, I. D. (2023). Talabalarning ijodkorlik qobiliyatlarini rivojlantirish mexanizmini takomillashtirish texnologiyalaritalabalarning ijodkorlik qobiliyatlarini rivojlantirish mexanizmini takomillashtirish texnologiyalari: talabalarning ijodkorlik qobiliyatlarini rivojlantirish mexanizmini takomillashtirish texnologiyalari.
9. Эргашев А. М (2016). Аҳоли фаровонлигини таъминлашда оилавий тадбиркорликнинг ўрни ва аҳамияти Тежамкорликнинг концептуал асослари ва унинг ижтимоий-иқтисодий шарт-шароитлари.2/174, 254.
10. Бабаева, Н. М. (2021). Роль государственного регулирования в развитии инвестиционной деятельности страховых компаний.

11. Babayeva, N. M., & Gafurova, N. I. (2023). Relevance and importance of forming the economic and legal culture of future specialists. In *ICARHSE International Conference on Advance Research in Humanities, Sciences and Education AUSTRALIA, CONFERENCE https://confrencea. org JULY15th*.