IDENTITY ORCHESTRATION

1. INTRODUCTION

Identity orchestration is about identity management, and identity management it's a simple concept of how you manage what users can access and what they can do inside of an application. Going further into the details, we have the six As model, that represents identity management:

The six As

- **Authentication**
- **Access control**
- **Attributes**
- **Authorization**
- **Administration** or **governance**
- **Audit**

In simpler terms, identity orchestration allows organizations to centrally manage user identities and access controls, even when dealing with diverse systems and platforms.

Use cases for orchestration

1- One of the most common two use cases for orchestration is **modernization**, particularly when migrating applications to the cloud. This process is expensive and time-consuming, and orchestration simplifies this transition by providing a layer that abstracts the underlying complexities, making the migration smoother and more efficient.

2- The final use case involves **eliminating passwords**. As legacy applications often rely on password authentication, this is a problem due to phishing and breaches arising from weak credentials. Fortunately, there are excellent solutions available (pass keys, multi-factor authentication, and tokens). However, integrating these new technologies with old applications is a challenge. Again, the solution is the abstraction layer, that connects these modern authentication methods with legacy applications.

2. CHARACTERISTICS AND OTHER ASPECTS

Standards

The standards SAML, FIDO2, and OpenID Connect play fundamental roles in the field of identity management and authentication. SAML facilitates secure exchange of authentication data between identity providers and services, enabling single sign-on (SSO) and establishing trust in distributed environments. FIDO2 promotes passwordless authentication through public key cryptography, enhancing security and user experience by eliminating password reliance and offering more secure authentication methods. OpenID Connect provides a standardized framework for verifying user identities in web and mobile applications, simplifying the implementation of SSO and user authentication in a secure and consistent manner. These standards strengthen security, streamline authentication processes, and ensure a consistent user experience across diverse digital environments.

API's availability and Modern Identity

API availability and modern identity management practices are crucial aspects highlighted. The discussion emphasizes the importance of API availability in bridging legacy systems with modern identity solutions. Modern APIs, particularly RESTful interfaces, offer efficient and standardized ways to manage identity data, such as through protocols like SCIM (Simple Cloud Identity Management). By leveraging RESTful interfaces and standards-based APIs, organizations can streamline identity management processes, enhance interoperability, and reduce the complexity associated with older SOAP-based approaches. Additionally, the document underscores the significance of orchestrating different identity systems to create an integrated identity fabric. This approach enables organizations to aggregate various identity services behind a common abstraction layer, facilitating seamless authentication, account creation, and credential issuance across disparate systems. By embracing API-driven identity management and orchestration, businesses can achieve greater agility, security, and efficiency in managing user identities and access control in today's digital landscape.

Automation Aspects of Identity Orchestration

The automation aspects of identity orchestration streamline identity management processes, enhancing operational efficiency and user experience through automated coordination and execution of identity-related tasks. Runtime identity orchestration ensures seamless authentication, authorization, and data access in real-time, while administrative automation simplifies user onboarding, offboarding, and access provisioning. Sequence administration tools automate task flow to uphold security and compliance standards, while integration with identity providers facilitates seamless exchange of identity data. Data encryption and sovereignty measures automate sensitive information protection, ensuring compliance with regulations and bolstering data security. Overall, incorporating these aspects into identity orchestration practices strengthens security measures, protects user data, ensures regulatory compliance, and enhances overall data privacy and security within identity management processes.

Security Concerns and Segregation of User Information

Security concerns regarding the segregation of user information are effectively addressed through identity orchestration practices. By implementing this framework, organizations can establish regional boundaries for data storage and processing, ensuring compliance with data sovereignty regulations. Automation within identity orchestration facilitates the secure movement of user data, strengthens security measures, and mitigates privacy risks. Furthermore, identity orchestration enhances data privacy and security by automating processes such as encryption, authentication, and access control, thereby safeguarding sensitive user information. Additionally, automation streamlines compliance efforts, aids in regulatory alignment, and ensures adherence to data protection laws. Overall, integrating these aspects into identity orchestration practices bolsters security, protects user data, and enhances overall data privacy and security within identity management processes.

Simplicity vs Complexity

Simplicity in identity management enhances user experience through intuitive interfaces, streamlined integration, efficient workflows, and consistent practices, while complexity arises from managing diverse systems, customization needs, scalability challenges, and security concerns such as data breaches and evolving threats.

3. AUDITION AND EMERGING TOOLS

Identity Orchestration has some benefits when auditing the systems. Not only it respects the old auditing mechanisms, but it also centralizes them making easier the communication between them. This new Abstract Layer gives a deeper knowledge on the user activity throughout the whole providers of the system. It is fairly simple to implement and deploy the Identity orchestration as the record in one service has been setting the abstraction layer up in less than 10 minutes. However, for big companies the standard is live in five (Setting up the layer in 5 business days).

The emerging tools for identity orchestration vary from ethics, budget and scope of the system but can be add up in:

- Biometrics

- Mobile pass
- Hardware tokens
- Blockchain

It is also remarkable how the AI revolution also affects this sector, where investigations about automatic deployment, secure and watch over the systems and preventing threats are being held with the objective of easing up the process.