KuppingerCole Report

EXECUTIVE VIEW

by Anmol Singh | May 2019

Ideiio IGA

Identity Governance and Administration (IGA) is an important security and risk management discipline that builds the necessary foundation of any organization's IT security portfolio. ideiio, a spun out from IAM systems integrator ProofID, is a new vendor in the IGA space offering IGA functions targeted at mid-market customers to meet their basic IGA requirements with minimal effort and investment.

by **Anmol Singh**
asi@kuppingercole.com
May 2019

Content

Related Research

Leadership Compass: Identity Governance and Administration - 71135

Leadership Compass: Access Governance and Intelligence- 71145

1 Introduction

Identity Governance and Administration (IGA), often referred to as integrated identity provisioning and access governance markets concerns the IAM capabilities that broadly deal with end-to-end identity life-cycle management, access entitlements, workflow and policy management, role management, access certification, SOD risk analysis, reporting as well as access intelligence. As IGA becomes an important security risk and management discipline directly impacting the security posture of any organization, a lack of basic IGA capabilities can leave organizations exposed to risks originating from inefficient administration of identities and access entitlements, poor role management and lack of adequate auditing and reporting. These risks range from identity thefts to unapproved and unauthorized changes, access creep, role bloating, delays in access fulfilment, orphan roles and accounts, SOD conflicts leading to occupational and other internal frauds. Several incidents in recent past have emphasized the need to have better IGA controls for organizations of all sizes, across all industry verticals.

Identity Governance and Administration (IGA) products support the consolidation of identity information across multiple repositories and systems of record such as HR and ERP systems in an organization's IT environment. The identity information including user accounts, associated access entitlements and other identity attributes are collected from across the connected target systems for correlation and management of individual identities and user groups as well as roles through a centralized administration console.

The IGA products are primarily aimed at supporting the following activities in an organization:

- Automated provisioning and de-provisioning of user accounts across nominated target systems
- Synchronization of identity attributes and access entitlements related to user accounts and groups across the identity repositories
- Management of access entitlements and associated roles of users across the IT environment
- Configuration and enforcement of static as well as event-driven access policies for the accounts to access the IT systems and applications
- Allowing users to validate their access to systems and applications, reset the passwords and create new access requests using self-service options
- Verification and synchronization of user account passwords and other identity attributes from an authorized event and source across the identity repositories
- Reconciliation of access across the IT environment based on defined policies to ensure compliance and prevent SOD and other policy violations
- Supporting on-demand and event-driven user access certification campaigns to detect and mitigate access violations
- Auditing and reporting of access activities leading to critical information regarding service monitoring and optimization

The IGA market has witnessed several trends over the last few years including a major shift in the product strategy and development roadmaps to provide in-built support for cloud applications. These advancements to support the cloud integrations are majorly driven in two directions:

a) IGA vendors that have re-architected their products to offer an identity bridging capability to integrate with cloud providers using industry specifications. Some IGA vendors have partnered with speciality identity brokers to extend on-premises IGA capabilities to cloud applications. Such approaches are suitable for organizations with a decent on-premises IT footprint and requirements to support complex IGA scenarios for legacy on-premises applications.

b) IGA vendors that now offer a cloud IGA product that is cloud deployable with ready integrations with popular cloud applications as well as with standard on-premises applications. This approach is more suitable for organizations with a massive strategic focus on the move to cloud and looking at achieving the benefits of cloud IGA deployments such as shorter deployment cycles, faster upgrades and lower TCO in short term.

At KuppingerCole, we identify and group the core capabilities delivered by the IGA vendors primarily in two product categories: Identity Provisioning and Access Governance. The core capabilities within each of these groups are represented in the figure below:

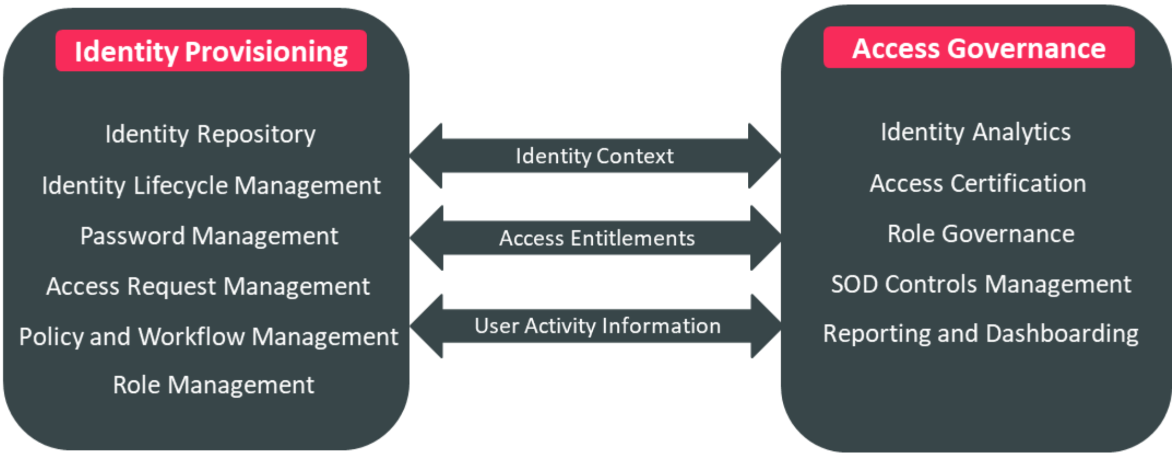

Figure 1: KuppingerCole Representation of core IGA functions

Besides these core functionalities, there are additional operational aspects that are considered to be important evaluating criteria for an IGA product or service and basically include capabilities such as UX (user experience), multi-tenancy, support for automation, high availability, ease of deployment, scalability and performance.

Please refer to **Leadership Compass for Identity Governance and Administration** for more details on the IGA capabilities discussed here.

2 Product Description

Ideiio is a new vendor in the IGA space; spun out from ProofID – an IAM professional services provider and system integrator based in Manchester, UK and Colorado Springs, US – ideiio builds upon the pre-existing and mature ProofID IGA product. ProofID has offered ProofID IGA as its primary IGA product for several years and has now segregated its software development activities from its IAM services portfolio in a new company called ideiio. This Executive View discusses ideiio's IGA offering which is targeted primarily at mid-market and B2B market segments.

The mid-market segment is characterized by unique IAM challenges that are very often ignored by large IAM solution providers. IAM requirements of mid-market organizations frequently fail to be on the list of primary design considerations for most (large) IGA vendors and it is increasingly brought to our notice that SMBs receive an inferior level of service and customer support in comparison to larger customers.

The IGA requirements of the mid-market segment vary significantly due to the needs of mid-market organizations to have simpler IGA deployments focusing on achieving low-cost IT efficiency. While resource availability remains a constant challenge for most mid-market organizations, the inadequate support and investment from business stakeholders for IT security adds to the growing challenges for IGA which remains one of the most expensive and complex security implementations.

The IGA capabilities offered by ideiio remain broad in scope but, unlike vendors targeting the enterprise space, relatively limited in the depth of functionality in a way that is suitable for most SMB organizations to meet their generic IGA requirements while allowing for easier and faster deployment, thereby delivering the desired time to value proposition.

Since the unique IGA challenges of small and medium-sized organizations result into non-uniform adoption of IGA technologies across organizations, there's a growing need and hence the market for IGA products and solutions that cater to simpler IGA needs and the unique IGA challenges of mid-market organizations. ProofID with its more mature IAM professional services and systems integration expertise offers ideiio as its IGA product and managed service (IDaaS IGA) targeted at generic IGA needs of the mid-market segment in the region, particularly of the higher education industry.

Ideiio is designed and developed to meet the IGA requirements of mid-market organizations and has achieved notable success in B2B implementations. Ideiio with its 'identity bridging' architecture aims to offer a simpler and faster deployment cycle for common IGA use-cases across most mid-market organizations. Ideiio is available in both software and virtual appliance formats and is also delivered as a managed service by ideiio hosted in AWS cloud. Designed to be multi-tenant, ideiio is a suitable choice for third party IAM professional service providers to host and offer managed IGA services.

Ideiio primarily comprises of two modules – the 'ideiio core' that serves as the main provisioning engine and the 'identity portal' that provides the self-service and access request management features. Build to support role-based access control, ideiio offers good support for defining and managing access entitlements for role creation and identity provisioning. The out-of-the-box delegated administration feature from ideiio allows management of the end-to-end process of requesting access through the ideiio user interface (UI) by both end users and delegated administrators.

Built upon Java and J2EE architecture framework, ideiio identity bridge is included as part of the core product and integrates out-of-the-box (OOTB) with the most available data source and repository types including LDAP, AD, SQL DBs, SCIM, REST APIs and other flat files (CSV) as identity stores for identity data synchronization. ideiio can act as an identity store or readily integrate with others.

Ideiio offers SCIM connections natively to most common target resources including SaaS applications through. However given the lack of current proliferation of the SCIM, the ideiio 'identity bridge' provides a means of extending connections to non-SCIM enabled cloud applications and infrastructure. The ideiio identity bridge currently supports SCIM 1.1, JDBC, LDAP, AD and CSV integrations. An SDK is available for the development of custom connectors for non-standard applications and target resources.

The ideiio Identity Portal provides a self-service interface for access request and approval management for end-users which is designed to be user intuitive .ideiio offers resource and application cataloguing for access request management. The cataloguing is role-based, thereby allowing users to only see and request access from a list of pre-approved resources and applications that they should be entitled to. Support for application entitlements allows ideiio to define and manage user's access at a fine-grained level for individual applications. Ideiio also supports basic segregation of duty (SoD) checks based on defined policy rules. Advanced identity and access intelligence features to support risk-based analytics or advanced segregation of duty (SoD) analysis are, however, not yet supported by ideiio but are featured on the mid-term product roadmap.

An application-based certification capability is currently under development and will be available as part of the upcoming ideiio certification portal in July 2019. The proposed certification portal will offer access governance capabilities including access certification feature.

Ideiio offers identity governance fundamentals which is mostly achieved through the use of out-of-the-box workflows and in-built reporting. Though reporting is limited, there's provision available to create and schedule custom reports and also to personalize the dashboard to feature required user and application parameters for easy monitoring.

Ideiio offers bi-directional OOTB integration with Ping Identity for access management. Ping Identity with its multiple authentication methods offers MFA for users. The integration, particularly with Ping Federate, offers means for exchanging authentication information, user attributes and access entitlements for a fine-grained authorization to the requested application or resources whether on-premises or in the cloud. ideiio also provides a provisioning integration for Okta via the Okta API.

With a good range of baseline identity life-cycle management and access governance features, ideiio makes a good choice of technology for the mid-market segment. Whilst the majority of its IGA product business is currently in the UK and neighbouring countries, ideiio is actively expanding its IGA business in the US, through its development and operational facility in Colorado Springs, CO. ideiio plans to include advanced support for identity analytics, SOD controls management and access governance in future product releases, targeted primarily at enterprise customers with a need for baseline IGA capabilities, to enable its customers to detect and prevent identity thefts more effectively.

With the options to be deployed in public cloud (AWS) for IDaaS IGA, ideiio offers the flexibility to be deployed in a private cloud or on-premises environment in a multi-tenant fashion, depending on the customer's deployment preferences.

3 Strengths and Challenges

Ideiio is primarily aimed at mid-market customers and offers a solution that covers most aspects of IGA preferred by SMB organizations to jump-start their IAM journey. Offered as a public cloud service hosted in AWS with the option of on-premise deployment, ideiio addresses generic IAM requirements around identity lifecycle management including identity fulfilment, password management and access governance in one product. Its 'identity bridging' architecture approach requires additional components to be installed but facilitates faster and easier deployment options for customers to onboard IGA without much efforts required from the integration and service delivery teams.

Combined with a good understanding of IGA requirements for mid-market customers owing primarily to its IAM professional services heritage from ProofID, ideiio offers good coverage of fundamental IGA features to meet the distinct and emerging IGA requirements of mid-market. With a strong presence in the Higher Education vertical ideiio's technology and inbuilt workflow templates are particularly well aligned to the IGA requirements of this sector. It also finds appropriate relevance within mid-market B2B use-cases due to its easy deployment approach and configurable options. Ideiio proposes a well thought-out product roadmap through 2020 to enhance ideiio and deliver more advanced IGA capabilities targeted at improved user experience, integration, standards support and access governance.

We expect ideiio to present a viable alternative to several prevalent IGA vendors for SMBs to meet their distinct IGA requirements in the near future. As ideiio becomes established as an IGA vendor, mid-market organizations, especially higher education institutions should consider leveraging on its industry expertise and experience.

Strengths	Challenges
● A focussed approach to IGA for addressing mid-market IGA requirements ● The Java-based architecture allows flexibility and easy skills availability for customization ● 'Identity bridging' approach enables easy extension into cloud and partner networks ● Early focus on open standards support makes it agile and a forward-looking IGA product ● Good market understanding with years of IAM systems integration experience ● A well thought out product development roadmap ● A channel-first approach builds trust and empowers partner ecosystem	● Limited technology integrations and partner ecosystem ● A weaker but rapidly building brand awareness ● Lack of identity analytics and access governance features

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com