KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | November 2017

Atos DirX Identity

Atos DirX Identity is a mature offering for IGA (Identity Governance and Administration), delivering both leading-edge Identity Provisioning capabilities and a strong Access Governance feature set. Atos has made significant improvements when it comes to the ease and flexibility of customization and added a modern, responsive user interface.

by **Martin Kuppinger**
mk@kuppingercole.com
November 2017

Content

Related Research

Executive View: Atos DirX Identity V8.5 - 70896
Executive View: Evidian Identity & Access Manager - 70871
Leadership Compass: Adaptive Authentication - 71173
Leadership Compass: Access Management and Federation - 71102

1 Introduction

IAM (Identity & Access Management) today is at the core of enterprise IT infrastructures when it comes to protecting digital corporate assets. IAM, as the name states, is about managing identities and their access. This involves managing user accounts and their entitlements across the variety of systems and applications in use in organizations.

Over the past several years, organizations have been facing multiple changes affecting their security posture. The perimeter which separated the internal network from the outer world does not have the same relevance it had before, with mobile users accessing internal systems, with integrating business partners and customers into business processes, and with the shift to cloud applications. On the other hand, the value and relevance of digital corporate assets and intellectual properties have increased. With the shift to connected things and to smart manufacturing, digital assets are becoming "crown jewels" even for more traditional businesses such as mechanical engineering.

Protecting digital assets, the systems, and applications in an IT environment of growing complexity and of a hybrid nature while facing ever-increasing attacks, involves several actions organizations must take. Protecting against internal and external attackers requires a well-thought-out understanding of risks and countermeasures.

Among the core elements of every infrastructure, we find IAM. IAM done right ensures that identities, their user accounts and passwords, and their access entitlements are well-managed. IAM thus reduces the attack surface by helping organizations moving towards the "least privilege" principle. IAM provides the tools to automate processes around managing users and access entitlements, but also for regularly reviewing these and identifying, e.g., excessive entitlements.

On the other hand, IAM also plays a vital role for business enablement, when it comes to the need of employees, contractors, business partners, and customers to access certain applications, systems, and data. IAM is the tool for implementing the workflows and automated processes for onboarding users and granting them access. Again, if done right, IAM can enable organizations by optimizing the onboarding and change processes, but also ensure that entitlements are revoked, and accounts are deleted or deactivated once they are no longer required.

Under the umbrella of IAM, we can differentiate between the "core IAM" or– as it is called frequently today – IGA (Identity Governance and Administration), and the broader definition of IAM which includes additional capabilities such as Privilege Management, Web Access Management, Identity Federation, and more. IGA, in fact, is an umbrella term for the two core elements of IAM, which are Identity Provisioning and Access Governance. Identity Provisioning supports automating processes for creating and managing user accounts and their high-level entitlements across the variety of systems and applications in use, while Access Governance adds the governance layer for analyzing entitlements, regular reviews and recertification, and also efficient access request workflows.

These core capabilities of Identity Provisioning and Access Governance frequently are available in combined products or in suites with a good level of integration between the various technical components. For the Access Governance part, it is essential for supporting the cooperation between

business and IT. Business requests and approves the relevant access, which must be mapped to technical entitlements. Creating that interface well, from the definition to the ongoing management and reviews of entitlements, is challenging. Furthermore, tools must support requirements such as Segregation of Duties controls, but also have insight into high risk combinations of entitlements.

Having an infrastructure for Identity Provisioning and Access Governance in place is the cornerstone for successfully managing identities, their accounts, and their entitlements across the heterogeneous and increasingly hybrid IT infrastructure of organizations. Enabling and protecting the Digital Transformation requires IGA.

One of the vendors in that space is Atos. Atos is the largest European IT service provider and amongst the global top 5 players for digital services. As part of their portfolio, Atos delivers various IAM services and products. Amongst these, there are the DirX products, including DirX Identity as an IGA offering. That also means that there are two IGA offerings, the Evidian and the Atos product. Customers are well-advised to discuss the best strategic choice for them thoroughly with Atos/Evidian.

2 Product Description

DirX Identity is a product that has a long history, dating back to the early years of IAM, when – at that time owned by Siemens – the first meta-directory solution had been brought to the market. Since then, the product has evolved massively, now being a comprehensive IGA solution that covers both Identity Provisioning and Access Governance. Over the past years, not only a variety of features has been added such as support for Access Recertification and Access Risk Management, but also the user interface has been modernized. In its current release 8.7, DirX Identity delivers to all major feature areas we expect to see in IGA products.

The foundation for these services are provided by strong Identity Provisioning capabilities, combined with the meta-directory approach. The latter supports customers in managing identity data from various sources, which is one of the major challenges in virtually all IAM projects. Data from various sources must be mapped, cleansed and consolidated. The rock-solid data management capabilities of DirX Identity support in this task.

DirX Identity also comes with a strong set of connectors, both regarding the breadth of supported systems and the depth of integration with these systems. A specific strength is the broad support for vertical solutions such as PLM (Product Lifecycle Management) or healthcare solutions, but also horizontal integration into smartcard management systems, physical access control, and unified communications. DirX Identity here benefits from both its origins at Siemens and the solution focus of Atos. The strong integration capabilities include strong and deep integration into various SAP systems, well-beyond what is found in some of the other products in the market. In the past releases, Atos has started adding cloud service support to its list of connectors, now supporting a number of such services out-of-the-box and also delivering RESTful API support for custom integrations.

Based on that foundation, DirX Identity supports both RBAC (Role Based Access Management) and rules-based approaches for managing access entitlements. Again, the product has a long history in that area and supports a broad and proven set of capabilities. A specific strength is the support of

parameterization of roles, which allows to create a standard role e.g. for “sales”, which then can be automatically “multiplied” for different sales regions with varying entitlements. Thus, the effort for managing related roles can be massively reduced. Roles can be assigned based on the context of users. Role hierarchies are supported as well.

DirX Identity also supports SoD (Segregation of Duties) controls between different roles, groups, and permissions. SoD controls are defined via policies and automatically enforced during the assignment of roles, groups, or entitlements. If a SoD violation occurs, a workflow for getting (or denying) approval is started. Policies are also used for defining other types of access assignments, beyond the role-based access control. They are specifically important for automated assignments of entitlements, particularly in the process of on-boarding new users. In sum, the features provided by DirX Identity in this area are comprehensive and mature.

One of the fields where we have observed massive progress of DirX Identity over the past years is workflow support. Aside of pre-configured workflows for access requests, access approvals, access recertification, or role lifecycle management, workflows also can be customized using a graphical workflow editor. Based on web services, DirX Identity and the workflows also can be seamlessly integrated with external ITSM (IT Service Management) tools and other services. Such integration is essential, given that – despite a broad set of connectors – many systems will never be directly connected, but manually managed. By using DirX Identity in conjunction with ITSM tools, all access requests, approvals, SOD policies, etc. can be managed in one central tool, which then sends requests for manual fulfillment to the ITSM tools. Such integration is the recommended best practice for setting up IGA solutions.

Another set of new features has been added around risk assessment andclassification. DirX Identity supports risk scoring for various objects such as accounts, groups, etc. Based on these, compound risk scores are calculated, and risk level of users are displayed. This e.g. allows for focusing recertification activities on high risk users that accumulate more access rights than others.

However, the biggest change comes with the new user interface (UI) that has been released with version 8.7. The UI and its customization has been, aside of the formerly limited workflow support, one of the major criticism of customers. With the enhanced workflow capabilities that have been added over the past years and the recent introduction of a new UI, DirX Identity provides state-of-the-art capabilities in this area. The new UI follows a responsive UI design approach. Based on HTML5 and consuming the comprehensive RESTful APIs exposed by DirX Identity, it runs on a variety of devices. Furthermore, there is a native Apple iOS app available. The new UI delivers out-of-the-box support for the common, user-centric scenarios such as access request and approval or recertification. Due to its conceptual approach, it can be easily customized, as well as customers can create own integrations based on the RESTful APIs. With the new release, Atos catches up with other vendors in the IGA market.

Notably, DirX Identity comes with exceptional high availability (HA) support, but also support for load-balancing between various instances of the DirX Identity servers and other capabilities. Again, there are various enhancements in that area, which allow to overcome restrictions in earlier releases regarding e.g. the performance for high workloads.

3 Strengths and Challenges

DirX Identity is a proven solution, but Atos has well-managed to modernize the tool and bring it to the level of current standards of IGA tools, with some areas of specific strength. Amongst these areas count the depth of connectors, the underlying support for identity data management based on the meta-directory capabilities, the high availability configurations, and the strong rule-based and role-based capabilities for managing access controls.

From a feature perspective, DirX Identity comes as an offering that delivers a comprehensive set of capabilities, with significant improvements made over the past years regarding the ease of customization and the overall flexibility of the offering. DirX Identity counts amongst the strong IGA offerings in the market.

The biggest question marks come from a go-to-market perspective and the small number of partners aside of Atos. However, Atos is able to deliver on global scale.

Strengths	Challenges
• Strong set of connectors, regarding both breadth and depth • New, modern UI based on a comprehensive set of REST APIs • Strong capabilities for both role-based and rule-based management of entitlements • Leading-edge high availability capabilities • Comprehensive support for all major IGA capabilities • Good workflow capabilities	• Limited visibility of the offering in the market and main emphasis on existing customers and support of integrated Atos solutions • Relatively small partner ecosystem aside of Atos, but delivery on global scale through Atos

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 global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

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