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 risk-based 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 together with RESTful interfaces.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

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, delivered by the Evidian business unit of Atos.

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 8.9, DirX Identity delivers to all major feature areas we expect to see in IGA products. This product is complemented by DirX Audit for advanced Access Analytics & Intelligence, and DirX Directory as an enterprise-grade directory service supporting DirX Identity.

The current release has been expanded in various areas over the feature set provided in earlier releases. While the previous changes focused on improving the UI and simplifying customization, the latest release comes with major changes in two areas:

1. The Business User Interface, i.e. the UI for non-administrative access, has been extended. This specifically affects approvals, which now are simplified and centralized, and delegation features.
2. The REST interfaces have been extended, specifically for enhanced and simplified integration to cloud services such as SaaS applications. They now enable integration into additional services and the use of the SCIM standard for provisioning to such services.

Aside of that, it delivers a couple of additional extensions such as an extended connector to Salesforce and changes to the underlying platform, i.e. Java versions, middleware, etc. Atos intends adding further connectors to cloud services in upcoming releases, beyond the list of currently supported capabilities.

The foundation for these services is 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. Atos provides various connectors for cloud services already, and continues enhancing both the breadth and depth of such connectors. As previously mentioned, various new capabilities in the recent release are targeted around supporting and integrating cloud services.

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 such as ServiceNow, 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 and classification. 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.

Since the update of the DirX UI, specifically the Business User Interface, both usability and customization have massively improved. Together with the enhanced workflow capabilities that

have been added over the past years and the current UI, DirX Identity provides state-of-the-art capabilities in this area. The UI of DirX Identity 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 UI delivers out-of-the-box support for the common, user-centric scenarios such as access request and approval or recertification. As previously mentioned, the UI has again been enhanced significantly, adding new capabilities and simplifying common processes. Due to its conceptual approach, it can be easily customized, as well as customers can create own integrations based on the RESTful APIs.

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.

Furthermore, DirX Identity is part of a broader ecosystem of solutions. Aside of DirX Access, which provides strong Access Management and Federation capabilities, there are DirX Directory as the underlying LDAP directory services, and DirX Audit providing extended Access Analytics and Intelligence. Both solutions can work in seamless integration with DirX Identity and are also continuously updated.

For DirX Audit, major changes include support for multi-tenancy and extended access policies, but specifically also a broader range of supported reports and better configurability of reports.

For DirX Directory, major changes include an enhanced LDAP Proxy that provides leading-edge Virtual Directory capabilities, and IoT related extensions, specifically regarding more granularity in access controls. Also, monitoring capabilities have been extended significantly. With these capabilities, DirX Directory rates amongst the strongest offerings in the market for Directory Services.

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

- Strong set of connectors, regarding both breadth and depth, including SaaS connectors, and good integration capabilities for further services

- 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

- Broad set of REST APIs for customization and integration

- Integrates tightly with additional solutions, including DirX Directory and DirX Audit

Challenges

- 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

- Administrator UI does not keep track with changes to Business User Interface

4 Related Research

[Executive View: Atos DirX Access - 80167](#)
[Executive View: Evidian Identity & Access Manager - 70871](#)
[Leadership Brief: 10 Top Trends in IAM – 80355](#)
[Leadership Brief: Identity Fabrics – Connecting Anyone to Every Services – 80204](#)
[Leadership Brief: Access Reviews Done Right - 80195](#)
[Leadership Compass: Identity as a Service (IDaaS) IGA – 80051](#)
[Leadership Compass: Identity Governance & Administration – 71135](#)
[Leadership Compass: Identity Provisioning - 71139](#)

Copyright

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

KuppingerCole Analysts, 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.