KuppingerCole Report

WHITEPAPER

By Martin Kuppinger
September 28, 2021

Making IAM agile and working to the business

IAM is changing. It is no longer about workforce IAM anymore, but about managing all types of digital identities, across a wide variety of use cases. Digital identities are at the core of digital business. Thus, modern IAM must be agile to cater to the ever-changing demand of the business, and serve every type of identities from consumers to devices, things, and services. This requires rethinking traditional approaches, having a holistic approach for IAM, a strong IAM organization, and modern customization and deployment approaches such as GitOps.

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

Content

Commissioned by iC Consult

1 Executive Summary

The role of IAM has changed fundamentally over the past decade. IAM today is way more than an administrative tool and a solution for enforcing Access Governance. Digital identities are at the core of the digital business. Consumers, customers, the devices and things they are using, business partners, but also services: The IAM focus of today goes well beyond employees and even beyond humans.A lack of ability in managing digital identities and their access, i.e., a lack in having a modern IAM in place, will hinder the digital business. Modern IAM and the ability to handle digital identities is essential for success not only in the initial Digital Transformation, but for continuous improvement of the Digital Business.

IAM thus must become agile and cover way more capabilities than ever before. And it must be ready when the business demand arises, not becoming a hindrance in the evolution of the Digital Business. This requires different, innovative approaches to IAM, including the way IAM is adapted to new demands. On the other hand, being an essential foundation for Digital Business, IAM must be reliable and stable. This involves approaches for adaptation and extension of IAM for delivering new capabilities to the demand.

Modern as-a-service deployment models and the growing number and maturity of standards help in reducing complexity and increasing agility. However, there is more required: A plan, an architecture, and an efficient approach for delivering new capabilities, integrations, and custom capabilities. IAM agility is based on the ability to serve new requirements fast and efficient within a defined framework. IAM agility is based on six pillars:

- Organization
- Model
- Plan
- TOM (Target Operating Model)
- Extension & Customization
- Integration

The areas of TOM and the ability of flexible extension and customization converge into the rather new concept of GitOps. Git emerged as a term for a software for distributed version control, which emerged into code management platforms. DevOps, as an established concept, combines development and operations by delivering software to operations in a continuous process. GitOps extends this concept by utilizing the concept of infrastructure as code (IaC), where the configuration of infrastructures is done as part of the code. Thus, within such model, not only customizations are provided, but as part of the GitOps approach, the configuration of the runtime environment is also managed in code. GitOps is an essential model for efficient operations of an agile IAM that is able to quickly serve new business demands. Service Layers is one of the still very few solutions, aside of pure IDaaS solutions, that consequently implement the GitOps paradigm for efficient IAM delivery and operations.

2 Highlights

- The need for a modern IAM: IAM becoming a business enabler, beyond just being an administration, security and governance tool
- The need for supporting all types of identities, beyond humans, and for delivering new capabilities as business demand arises
- How to avoid IAM for sprawling despite new business demands and the need for delivering a way broader set of capabilities
- Essential elements for a modern IAM organization and tooling
- APIs and modern architectures as a cornerstone for agile IAM
- The need for GitOps: Integrating development, deployment, and operations for continuous delivery and seamless operations
- The Service Layers approach on agile IAM and GitOps
- Recommendations for moving towards a modern, agile IAM

3 Changing business demand: IAM becoming a business enabler

IAM is a business enabler. Digital identities are at the core of every digital service, and digital business relies on digital identities. Thus, the scope of IAM must be redefined, well beyond workforce IAM.

Going back some ten years, IAM (Identity & Access Management) was still a technical solution, helping administrators in managing users and their access and in increasing access security, and supporting risk managers in complying with various regulations, particulary by doing regular access reviews. The focus back then was on employees.

Since then, the role of IAM has changed fundamentally. Digital identities are at the core of the digital business. Consumers, customers, the devices and things they are using, business partners, but also services: The IAM focus of today goes well beyond employees and even beyond humans.A lack of ability in managing digital identities and their access, i.e., a lack in having a modern IAM in place, will hinder the digital business. Modern IAM and the ability to handle digital identities is essential for success not only in the initial Digital Transformation, but for continuous improvement of the Digital Business.

Digital Identities are as essential to the success of the digital business as IoT, AI, or data.

Digital Identities are, at the level of IoT (Internet of Things), AI (Artificial Intelligence) or data, one of the (few) essential enabling technologies for the Digital Business.

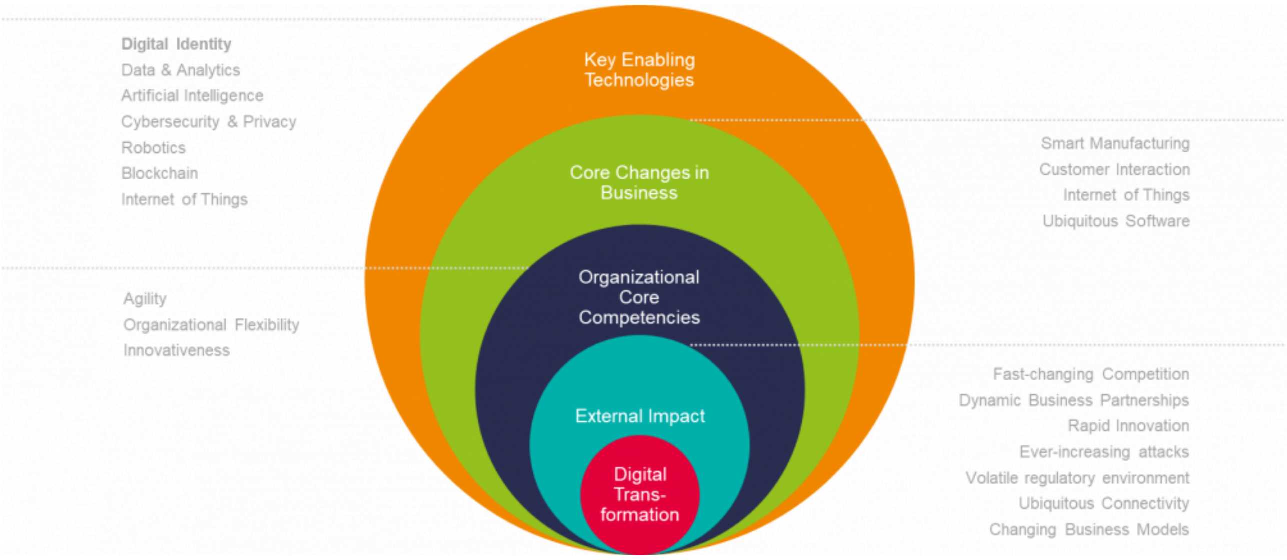

Figure 1: Digital Identity must be a main element of every Digital Transformation and Digital Business initiative.

With the need for organizations to be way more agile than in ancient times, for continuous innovation, highly volatile partnerships, and direct interaction with customers, as well as for the need to support connected things and devices and their relationships to the users, IAM also must become way more agile than before.

IAM must become agile and cover way more capabilities than ever before. And it must be ready when the business demand arises, not becoming a hindrance in the evolution of the Digital Business. This requires different, innovative approaches to IAM, including the way IAM is adapted to new demands. On the other hand, being an essential foundation for Digital Business, IAM must be reliable and stable. This involves approaches for adaptation and extension of IAM for delivering new capabilities to the demand.

4 The challenge: Delivering new services now, without IAM sprawling

With the need for delivering a way broader set of IAM capabilities than ever before, and the need to cater to new business demands to IAM in an agile manner, the art is to avoid sprawl and still deliver consistent IAM services in an efficient manner.

The challenge of the IAM evolution is in that it is multi-dimensional, across three different axes:

- Identity types: From employees to other human identities such as partner and customers, but beyond that to non-human identities such as things, devices, or services
- Deployment & operating models: From on-premises deployments, managed by the internal team, to IDaaS (Identity as a Service) and managed service deployments
- Capabilities: From traditional user lifecycle management, identity provisioning, access reviews, or federation to managing resource entitlements in multi-cloud, multi-hybrid environments, password-less authentication, and decentralized identities

With business demand for supporting new use cases such as consumer identities with effortless onboarding, identity vetting, or simple yet secure authentication, for running and securing SaaS services, or for securing the agile DevOps environments spanning multiple clouds, there is a risk that IAM solutions are implemented as point solutions, based on specialized but non-integrated technologies, or even by other departments such as marketing (for consumer-centric solutions) or decentral developer teams for their specific use cases.

This is not saying that there must be one big, monolithic IAM solution. This would not work and would not exist. But coordinating and streamlining initiatives, and consolidating efforts into a holistic strategy and architecture is essential to avoid later integration and management challenges, and to reduce overall cost for IAM.

It is even that "big bang" approaches where large, complex solutions are deployed in multi-year projects are fostering sprawl, because IAM will not be able to deliver on time to the business demand. The art is to increase agility of IAM deployments and consolidating efforts, while avoiding sprawl.

Successful IAM organizations must manage to get ahead of the curve, not following the business demand but being prepared to deliver when new capabilities are required.

It is about getting ahead of the curve. Traditional IAM is not known for delivering fast and efficiently to new demands. There are reasons for that:

- Traditional IAM solutions, specifically IGA (Identity Governance & Administration, i.e., User Lifecycle Management, Identity Provisioning, and Access Governance) have been commonly delivered as relatively complex and monolithic on-premises solutions with a high effort in customization.
- IAM, as an integration technology, carries the burden of technical integration with a vast range of different technologies. Specifically, integration into legacy environments such as SAP ERP or mainframes, but also homegrown applications have contributed to the complexity.

Modern as-a-service deployment models and the growing number and maturity of standards help in reducing complexity and increasing agility. However, there is more required: A plan, an architecture, and an efficient approach for delivering new capabilities, integrations, and custom capabilities. IAM agility is based on the ability to serve new requirements fast and efficient within a defined framework.

5 The solution: Modern architectures, legacy IAM integration, services

Modern architectures, target operating models, and deployment models are the foundation for a successful IAM delivery. However, this requires an adequate organization, a unified perspective on IAM, and a plan, as well as the backwards compatibility to legacy IAM.

IAM agility is based on six pillars:

- Organization
- Model
- Plan
- TOM (Target Operating Model)
- Extension & Customization
- Integration

Modern, agile IAM requires a well-defined **IAM organization**. With the importance of digital identities and thus also IAM for the digital business, there is a need for a distinct IAM organization. IAM is not just an element of cybersecurity or IT infrastructure. This also means that there must not be split responsibilities for different elements of IAM such as customer vs. employee IAM or on-premises vs. cloud IAM. While there must be a defined collaboration of the central IAM organization with decentral entities, be it functional entities, regional entities, or legal entities, ownership of all IAM must become centralized.

Second, there must be a defined, unified **model** for IAM. One established model is the KuppingerCole Identity Fabric, which gives a comprehensive perspective across IAM capabilities and services, enabling seamless yet secure and controlled access of all types of identities to all types of services.

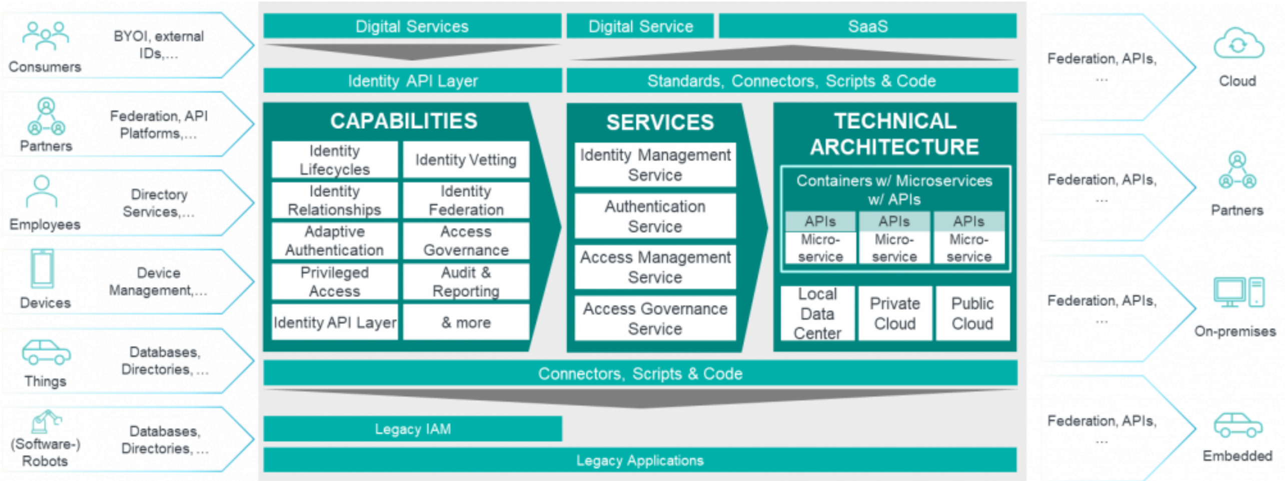

Figure 2: The KuppingerCole Identity Fabric is a paradigm delivering a unified perspective on IAM across all areas.

Defining such a model is an essential task for being able to deliver to the business demand on time. Such model allows for adding new capabilities, and to quickly identify whether a demand can already be covered by existing services.

One of the biggest challenges is planning. Ideally, IAM is able to cater to the business demand once that arises. In practice, this will not always work. Some capabilities are foreseeable, other will be reusable for other purposes. There needs to be a **planning**, taking into account both current requirements and the trends and foreseeable future requirements. Based on that, a roadmap can be defined. But even with the best planning, there will arise new demands that must be supported short-term. A model helps in understanding how new requirements fit into the overall IAM architecture and tooling. But plans then will change. Agile planning approaches for IAM, split into the "now, soon, later" phases, helps for IAM to serve also to short-term demands, within the defined framework and backed by agile deployment methods.

The **TOM (Target Operating Model)** is an important foundation. Rapid deployment of new capabilities only will work in a modern TOM, with as-a-service deployments of solutions in a modern architecture. Modern architectures are based on elements such as microservices architectures, container-based deployments, and APIs (Application Programming Interfaces). They stand in stark contrast to the traditional, monolithic, and thus inflexible architectures frequently found in established IAM tools. The TOM defines both the deployment and operation.

Modern architectures, supporting APIs, being based on microservices, and enabling segregation of custom code via APIs are essential for rapidly delivering the required customization, integration, and orchestration to the business.

The architecture also impacts the field of **extension & customization**. This requires a well-thought-out strategy to ensure that two conflicting targets are met: The ability to quickly customize, integrate, and orchestrate, and the ability to maintain software along its entire lifecycle. One of the frequently found challenges in traditional IAM deployments is that customizations tend to break with major updates, due to the fact that customizations frequently are tied deeply into the product. This can be avoided by utilizing APIs and having a defined Identity API layer, exposing the IAM services. On one hand, this allows for rapidly building new digital business services utilizing standardized IAM services. On the other hand, all customizations, integrations, and orchestrations can be isolated into separate microservices, using the Identity API layer and, if required, exposing own, additional APIs. Thus, as long as APIs remain stable, the custom code will not break.

Last not least there is the need for **integration**. While there is the new world of digital business services consuming identity APIs, and the SaaS services being managed by the modern IAM, there is also the need for supporting legacy IAM. This can be done by serving the legacy from modern IAM, but also by using existing IAM with a limited capability as interface to the legacy IT, integrated into the modern IAM. Such approach allows for a gradual migration at own pace.

GitOps is about an integrated approach of DevOps and Infrastructure as Code, ensuring that everything can be deployed and operated seamlessly.

The areas of TOM and the ability of flexible extension and customization converge into the rather new concept of GitOps. Git emerged as a term for a software for distributed version control, which emerged into code management platforms. DevOps, as an established concept, combines development and operations by delivering software to operations in a continuous process. GitOps extends this concept by utilizing the concept of infrastructure as code (IaC), where the configuration of infrastructures is done as part of the code. Thus, within such model, not only customizations are provided, but as part of the GitOps approach, the configuration of the runtime environment is also managed in code. GitOps is an essential model for efficient operations of an agile IAM that is able to quickly serve new business demands.

6 Service Layers: Delivering modern IAM as a service, built for GitOps

Service Layers delivers a modern IAM framework, utilizing existing IAM solutions, that build on the GitOps paradigm and thus overcomes the challenges of traditional IAM deployments.

Service Layers, part of iC Consult group, provides its own IAM framework that is built around existing, established IAM solutions. Service Layers on one hand delivers comprehensive IAM solutions as managed service in a modern TOM. On the other hand, Service Layers builds on a GitOps approach and exposes a consistent Identity API layer for customization, orchestration, and integration.

The approach chosen by Service Layers is based on a long-standing experience from the iC Consult practice.

The approach Service Layers has taken is based on the experience from the iC Consult practice in deploying and operating IAM, and is enforcing various concepts and delivering the required capabilities:

- IAM installations change over time with regards to the operational and functional requirements. Service Layers allows full-stack comparisons of different versions and configurations to continually optimize for current best practice and efficiency.
- Auditability of changes to the entire IAM installation, not only functional configuration, is critical to identify negative and positive changes to the system. A unified view of system changes and effects allows data-oriented comparisons and simplifies compliance reporting.
- When IAM components are designed as highly-available services, they can be added to an IAM installation without a reconfiguration of other components and infrastructure.
- Components should be self-managed whenever possible: Each component should provide metrics and associated charts, structured logs and associated reports. Metrics, charts, logs and reports should be discovered by monitoring and logging systems without manual reconfiguration of the supporting services.
- It is necessary to have repeatable approaches to high availability within each IAM component that matches the availability requirements and capabilities of the infrastructure. Managing infrastructure, application (IAM), and configuration together ensures alignment of all layers of the installation. The capability to expand installations to multiple data centers and geographies provides benefits for

performance (reduced latency), high availability and business continuity.

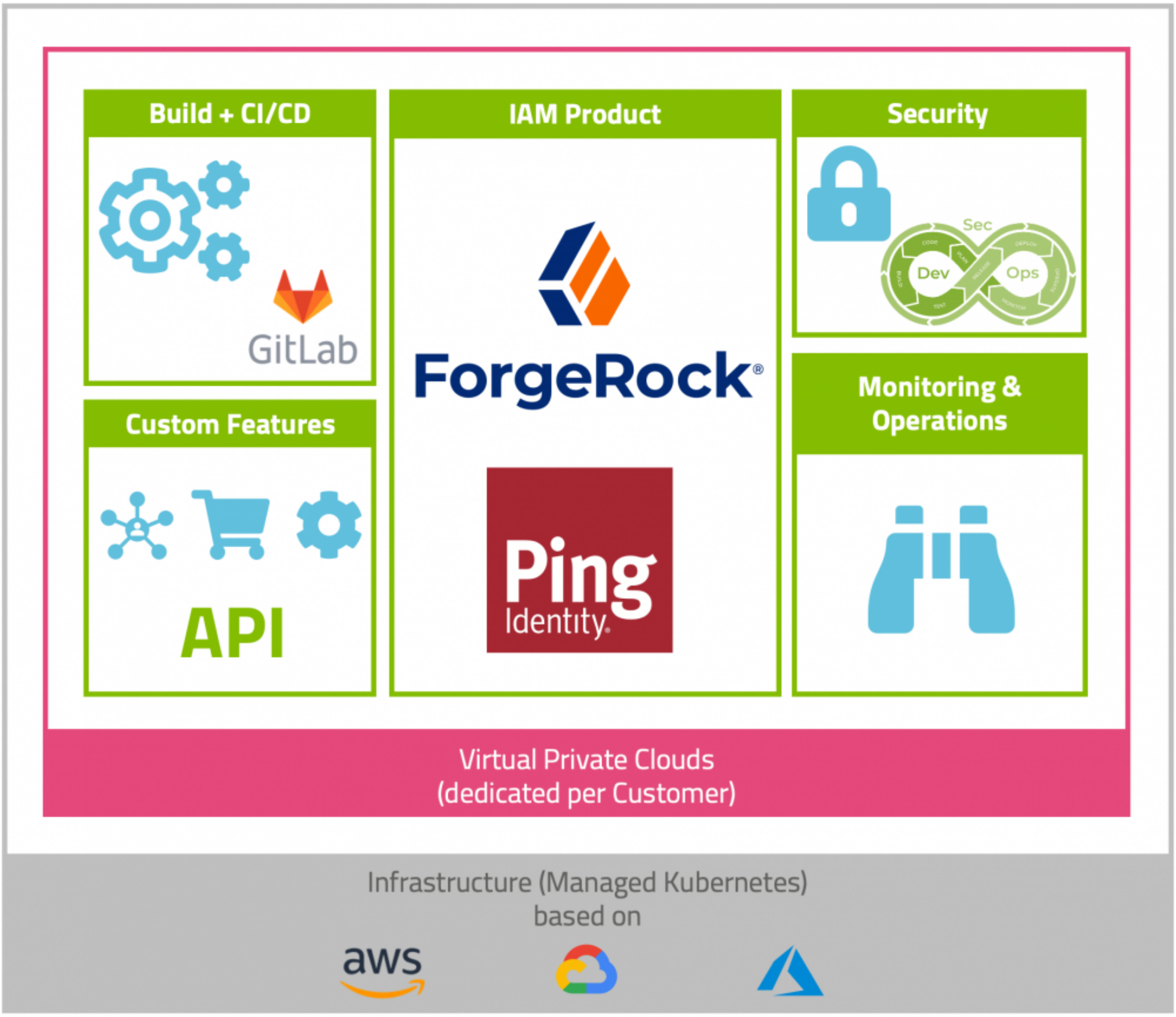

Figure 3: Service Layers delivers a solution that exposes a consistent Identity API Layer and is operated based on the GitOps paradigm(Source: Service Layers)

The target of this approach, based on the GitOps paradigm, is to deliver self-managed software components as part of both the standard deployment of Service Layers, and for the custom components to be added. This allows for automated and repeatable deployment on one hand across customers and instances, but also for a high degree of automation in delivering custom components and updates.

Utilizing GitOps allows for automated and repeatable deployments.

Given the fact that a significant part of major incidents in IAM operations stem from errors in deploying upgrades, such approach is essential for agile IAM deployment and operations. When incidents appear because, as frequently observed, some libraries and modules are just forgotten to be deployed during an upgrade, it is time to change. A modern IAM must not only provide the capabilities required by the business, but also come with a delivery and operations approach that serves the dynamic nature of today's IAM. Service Layers is one of the still very few solutions, aside of pure IDaaS solutions, that consequently implement the GitOps paradigm for efficient IAM delivery and operations.

7 Recommendations: 8 areas to cover for a truly agile IAM

Making IAM agile and ready to serve the demand of today's digital businesses requires to think beyond the traditional approach on IAM, in both scope and the way IAM is delivered in an organization.

IAM must become agile and comprehensive to serve the business needs in today's digital businesses, where digital identities are an enabler for delivering digital services that distinguish businesses in the competition. This requires more than just some new technologies such as IDaaS, but a comprehensive approach on IAM, covering eight areas:

- Organization: There is a need for a well-thought-out, centralized IAM organization and a model of working with decentralized IAM identities (e.g., regional) as well as other IT units such as the IT governance organization.
- Model: IAM requires a holistic perspective, such as the KuppingerCole Identity Fabric. This must cover all types of identities, all areas of IAM, and all types of services that access must be provided to. Such model will evolve over time and must allow to incorporate new capabilities.
- Plan: There is a need for a defined roadmap, but also the agility to adjust to newly arising business demands.
- Operate: Operations must shift to as-a-service, managed models that provide flexibility in deployment. The TOM (Target Operating Model) is an essential part of every IAM model.
- Build: The ability to customize, integrate, and orchestrate based on a modern architecture and a comprehensive set of APIs helps in reacting flexibly to new business demands, and to segregate custom code from the standard tools.
- Integration: IAM must support the entire multi-cloud, multi-hybrid environment, from modern SaaS services and the management of resources across clouds to the legacy IT environments. Thus, IAM must also provide a means for integrating back to the legacy.
- GitOps: With the need for deploying updates and new capabilities rapidly, the need for ensuring proper deployment and operation arises. It is time to think beyond DevOps and move to GitOps as the approach for managing custom code, standard components, and the runtime environment in a consistent and coordinated way.
- Education: Last not least, it is about people. Building a time and educating it is essential to success in IAM.

It is time to think beyond IAM as a set of technical tools, and to build an IAM organization and infrastructure that is ready to serve today's business demand.

8 Related Research

Whitepaper: IAM: Globalization & Large-Scale Enterprise

Executive View: Service Layers Managed IAM

Leadership Compass: Identity Fabrics

Leadership Brief: Leveraging Identity Fabrics on Your Way Towards Cloud Based IAM

Leadership Brief: Identity Fabrics - Connecting Anyone to Every Service

Content of Figures

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, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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