KuppingerCole Report

WHITEPAPER

By Warwick Ashford

May 12, 2020

IAM: Globalization & Large-Scale Enterprise

Identity and Access Management (IAM) has never been more important or challenging in the face of a rapidly changing business, regulatory and IT environment. This is especially true for multinational companies that must comply with an ever-increasing number of security and privacy regulations. Service Layers delivers a managed IAM service using a scalable, customizable, component-based platform with a service-oriented architecture to support multi-instance deployments to meet the key IAM challenges facing global enterprises.

By **Warwick Ashford**
wa@kuppingercole.com

Content

Commissioned by iC Consult

1 Introduction

In the digital era, the most significant trend is towards the provision and consumption of all IT as cloud-based services, including Identity and Access Management (IAM). As a growing number of workloads and IT services move to the cloud, it makes sense to move IAM to the cloud as well. Moving IAM to the cloud helps avoid the integration, management, and licensing complexity of hybrid IT environments where some workloads run on premise while others run in parallel in the cloud.

However, cloud-based IAM services will still need to support hybrid IT environments for the foreseeable future and at the same time will need to evolve to include support not only for employees, but also for business partners, customers, consumers and non-human entities that have identities that need to be managed, such as internet-connected devices that make up the Internet of Things (IoT).

Although a number of IDaaS (Identity as a Service) solutions have appeared on the market in recent years in line with the as-a-service trend, most of these have focused on some aspect of IAM, such as supporting Single Sign-On (SSO) or adaptive authentication schemes. However, IAM is about much more than just authenticating a user.

In addition to authentication, IAM is about managing identities and the entitlements attached to those identities as well as authorizing access. IDaaS solutions that do not cover all key aspects of IAM lack the depth that is required by modern enterprises to reduce security and compliance risk.

The shift of business workloads to the cloud, however, is a long-term journey for most businesses. Similarly, the shift from on-premises IAM to IDaaS solutions, while at the same time delivering comprehensive support for IAM capabilities across all target systems, regardless of their deployment model, is also a multi-step journey.

Running comprehensive IAM capabilities as a managed service is one of the viable options open to companies on that journey to a more modern IT environment because it caters for the IT reality, which will be hybrid for most companies in the short to medium term, while enabling a gradual transition to a future IT environment provided entirely by cloud-based services. In the interim, comprehensive managed IAM solutions also enable a high degree of customization that is typically required by multinational companies, while still being run as a service.

We recommend that manufacturers and other multinational companies consider switching their Identity and Access Management to a managed IAM service provider that enables them to meet the challenges of fulfilling organization-specific requirements, supporting complex hybrid environments, operating IAM

infrastructures in global environments, and allowing for a gradual step towards an easy-to-manage IAM, without any trade-off in depth and breadth of capabilities.

iC Consult subsidiary, Service Layers, headquartered in Germany with offices in Switzerland, Austria, Spain, UK, US and China, is one of the few players in the IDaaS market that provides scalable and custom managed IAM services with global support and based on market-leading IAM products

2 Highlights

- IAM is particularly challenging for global organizations in a rapidly changing business, IT and regulatory environment
- Delivering IAM services using different IAM technology stacks, processes and operating models leads to increased cost and poor efficiency because of difficulties with integration and consistency
- Digital Transformation is changing IT in businesses by driving the move towards the as-a-service model, where everything – including IAM - can be provided and consumed as a cloud-based service
- Consistent technology, processes, and operating model plus flexibility for local language and regulatory requirements are key to the success of global IAM
- Multinational companies should consider switching their IAM to a managed IAM service provider to meet the challenges of operating IAM infrastructures in global environments

3 IAM Challenges for Global Companies

Managing identities and access entitlements is becoming increasingly challenging in a rapidly changing business, regulatory and IT environment, but those challenges are compounded for multinational organizations due to the distributed nature of their operations and different local requirements.

Identity and Access Management (IAM) is especially challenging for medium to large multinational companies that need to manage the identities of employees, partners, customers, consumers, and devices wherever the company does business, while meeting various local requirements.

A global IAM capability is challenging because of the need for consistent management of identity and entitlements across the globe to enable and control access to cloud-based applications and data, to federated applications, and to legacy applications.

IAM presents specific challenges to multinational companies.

Within the broader IAM challenge, there are several other specific challenges facing multinational organizations such as:

1. Being able to deal with customers and employees with identities originally registered in one continent or region using their identities to access services and systems in another continent or region.
2. Delivering IAM services using different IAM technology stacks, processes, operating models, and maturity levels across the different company locations that typically leads to difficulties in integration and consistency requiring costly and time-consuming manual interventions.
3. Supporting different languages in the different regions/countries where the company operates.
4. Ensuring fast time to market for products and services requiring consistent IAM for employees, partners, customers/consumers in response to market needs/opportunities.
5. Achieving a custom fit for IAM services to meet the requirements of global and regional use cases.
6. Enabling fast, simultaneous rollouts for new applications to new markets.
7. Standardization and automation to reduce costs and risk of in-house solutions.
8. Built-in support for IoT, DevOps models and local DevOps teams.
9. Retaining control of infrastructure, changes, deployments, and interfaces.

10. Complying with specific regional and local regulatory requirements in addition to global regulatory requirements in terms of:

- Data protection
- Information security
- Product safety and quality assurance
- Critical infrastructure providers
- Export regulation
- Financial regulation.

IAM is a very common element to regulations, with each type of regulation often setting some requirements for managing IDs, onboarding, identification of customers, authentication, access control, and access governance. To deal with these regulations, multinational companies need a strong IAM that is flexible enough to be strong in some regions, but more relaxed in others.

4 Shift to as-a-service model

Digital Transformation is changing IT in businesses by driving the move towards the as-a-service model, where everything can be provided and consumed as a cloud-based service.

Digital Transformation is changing IT in businesses fundamentally by driving the move towards the as-a-service model, where everything and anything in the IT world can be provided and consumed as a cloud-based service. This means that the market is about to change fundamentally with fewer solutions available on premise. Organizations need to start preparing for that change by adopting a service-oriented approach to new products and implementations to ensure they are not blindsided by it.

Critical workloads are increasingly moving to the cloud, so it makes sense to move the management of those workloads, including Identity and Access Management (IAM), to the cloud as well to avoid the integration, management and licensing complexity of hybrid IT environments where some workloads are running on premise while others are running in parallel in the cloud.

Identity Management will inevitably move to the cloud

Cloud-based IAM also makes more sense in light of the trend of focusing increasingly on managing access at run time rather than setting identity governance and administration (IGA) parameters when deploying systems, even though this approach remains relevant, especially when it comes to IAM for employees. That said, organizations could begin their journey to service-based IAM by starting with an IAM project for employees, including migration of on prem IGA tools to microservices architectures, which would enable these microservices to run in various deployment models. However, there is a general trend towards the convergence of all use cases in identity management, which strongly favors the service-based approach at all levels. At an architecture level (microservices), at an application level (granular services that can be both exposed by the application and consumed via APIs), and at the broader cloud-based services level.

Identity is becoming one of the new, essential security perimeters

Any organization thinking about the future of identity should consider moving to a services-based architecture because digital transformation is changing the way business communication takes place, how people work together and how services and goods are created and delivered.

Identity Management plays a crucial role in enabling the creators and consumers of digital services to be able to access them from anywhere, using any device. The traditional network perimeter is disappearing,

with agile businesses using cloud services and mobile users connecting directly to partners, customers, and consumers. The notion of identity as one of the new, essential security perimeters is becoming a reality as traditional perimeter-based security becomes less meaningful in the context of digital transformation and the resulting digital workspaces that can be accessed from just about anywhere using a range of devices, and this means that identity Management also needs to be transformed into a set of services or even microservices that make it possible to make services available to all users everywhere in a way that is secure, scalable and managed.

Global companies are better served by global as-a-service models

	Consistent Technology	Consistent Processes	Consistent Operating Model	Flexibility for Localization	Global Scalability
On premises IAM run by company				✓	
On premises IAM with some managed service			✓	✓	
Fully managed IAM in company data center	✓	✓	✓	✓	✓
Fully managed IAM in private or public cloud	✓	✓	✓	✓	✓

Figure 1: IAM Deployment Model Matrix

5 Advantages of Identity as a Service (IDaaS)

IDaaS solutions offer several key benefits that could help multinational organizations to tackle the challenge of running a global IAM

Since first appearing on the market, IDaaS (Identity as a Service) solutions have gradually matured to include identity management, entitlement management, authentication and authorization, which are the key components of IAM, adding the depth required by modern enterprises to reduce security and compliance risk.

IDaaS delivers IAM benefits particularly for multinationals

The IDaaS market has registered significant growth in the past few years because of the ability of IDaaS to enable organizations to:

- Achieve better time-to-value proposition over on-premises IAM deployments
- Extend IAM capabilities to meet the security requirements of growing SaaS portfolio
- Adopt global IAM standards and practices with access to industry expertise
- Reduce internal IAM costs and efforts to keep up with the market trends
- Limit internal IAM failures in project delivery and ongoing operations.

Consistency is key to global IAM

In tackling the challenge of a global IAM, it is important to keep in mind that ultimately the purpose of IAM is to provide the means of connecting everyone to every service. This highlights the need for a consistent set of services that will enable the sharing of identities across services to allow access to the services required to work with employees and partners as well as integrate customers and consumers. All these entities need access to the cloud, to federated applications, and to legacy applications, but they typically use different types of identities.

The challenge, therefore, is being able to deal with the identities of:

- Customers/consumers who might be bring their own identity or use some external identity

- Business partners that may be federated in or come through some new service built using an identity API platform
- Employees which probably still reside in the company's own directory service

In order to create and manage accounts for each of these identity types as well as manage and control access rights with the appropriate level of governance and privacy, including consent management, most organizations will need to think about restructuring their IAM.

Global IAM is well-suited to a service-based model

Our approach is to use a service-based model and think about using a set of standardized and consistent services around the globe that can deliver as a utility all the identity services an organization requires, including registration, verification, governance, security and privacy.

For most businesses this will mean making fundamental changes to their IT architecture to become more agile and flexible by separating identity and applications, and providing the backend systems required to make all the necessary connections using Application Program Interfaces (APIs) that bridge services, microservices and containers in the cloud (public and private) and on premise.

These changes will result in a converged digital identity backend or "Identity Fabric" that refers to a set of connected enabling IT components that work together as single entity.

Identity Fabric is a concept for connecting everyone to all services

An Identity Fabric, therefore, is a concept, not a single tool, that is about connecting every user to every service and is centered around managing all types of identities in a consistent manner, managing access to services, and supporting federating external identities from third-party providers as well as the organization's own directory services.

The concept of Identity Fabrics refers to a logical infrastructure that enables access for everyone and everything from anywhere to any service within a consistent framework of services, capabilities and building blocks that are part of a well-defined, loosely-coupled overall architecture that is ideally delivered and used homogeneously via secure APIs.

Identify Fabrics are focused on delivering the APIs and the tools required by the developers of the digital services to support advanced approaches to Identity Management such as adaptive authentication, auditing capabilities, comprehensive federation services, and dynamic authorization through open standards like OAuth 2.0 and OpenID Connect.

The service-based approach is consistent with what is required to address the challenge of operating IAM global environments. Whatever approach you choose, it should ensure:

1. Consistent technology.
If there are different technology stacks in different locations, it will be difficult at best and impossible at worst to deliver good IAM services. Too many different technology stacks that often overlap inevitably leads to integrations problems, which is often costly and not conducive to delivering a reliable IAM with a good level of service.

2. Consistent processes
Despite the need for regional and local specifics, processes must work well across the entire organization. If processes are not consistent and integrated, things like staff relocation from one region to another will become difficult and cumbersome. Inconsistencies in the way IAM is done leads to massive problems and cost because it will result in inconsistent identity data that must be fixed manually.

3. Consistent operating model
The operating model must be consistent to ensure smooth, round-the-clock operation of the entire IAM system. This is easier to achieve when there is a consistent approach because there is only one operating model to implement.

4. Flexibility for localization
While consistency is key, there must be flexibility for regional and local specifics, such as language, processes, and regulatory requirements.

4.1 Regulatory compliance
IAM must meet the regulatory compliance requirements across the entire organization. IAM is a key element in every form regulatory compliance because there are always some requirements around access controls, authentication, and access governance.

4.2 Multi-language support
Global organizations need local language support, at least for the major regions in which the company does business.

All the above requirements are supported by the as-a-service model. A growing number of organizations are shifting their IAM to the as-a-service model in the short to medium term as a cost effective way of delivering an efficient global IAM that is flexible enough to meet local language, process, and regulatory requirements.

Key capabilities of comprehensive IAM services include:

- Support for existing Directory Services on premises and in the cloud
- Integration of all sources of identity information
- Connectors to a broad variety of target systems on premises and in the cloud
- Self-service facilities for things like password management and access requests
- Support for mobile interfaces to access key functionality
- Access request management and access review processes

- Segregation of Duties management and entitlement management
- Central administrative UI
- Strong set of APIs and support for hybrid IT environments
- Modern architecture based on microservices and containers

IAM as-a-service offerings that have all or most of these features provide a viable short to medium term option for organizations unable to move immediately to the cloud and a services-based model for IAM. Managed IAM services allow companies to deploy a modern, scalable IAM capability quickly and easily to benefit from a balance between customization and standardization, and faster roll out of applications and services using automated, standardized IAM processes.

We recommend that manufacturers and other multinational companies consider switching their Identity and Access Management to a managed IAM service provider that enables them to meet the challenges of fulfilling organization-specific requirements, supporting complex hybrid environments, operating IAM infrastructures in global environments, and allowing for a gradual step towards an easy-to-manage IAM, without any trade-off in depth and breadth of capabilities.

6 Service Layers: Delivering an IAM Managed Service with Global Support

Service Layers delivers a comprehensive managed IAM solution, based on best-of-breed IAM products and modern architectures.

Service Layers, a subsidiary of German system Integrator iC Consult, provides IAM deployments and operations in data centers in Germany, Austria, Switzerland, Spain, UK, US and China, and is one of the few players in the IDaaS market that provides global support for scalable and custom managed IAM services. Multinational companies operating in countries or regions where there are special data protection and other legal requirements, need to keep this in mind when choosing an IDaaS provider.

Core technology

Service Layers uses market-leading IAM products from Ping Identity and ForgeRock to provide core IAM functionality and distinguishing features such as:

- Multifactor Authentication (MFA), mobile authentication/authorization, and adaptive risk management and authorization
- Unified profiles that ensure all customer data is stored one place, is secured, is synchronized across all systems, can be accessed at scale, customer consent in enforced, and there a clear audit trail
- Extreme scale and performance for peak demands such as service roll outs to several markets
- Support for identities of partners, customers, consumers and non-human entities like IoT devices.

Employee and customer services include:

- Self-service portal and password management
- Profile management, and consent and privacy management

Other features include:

- Delegated admin portal for CIAM, business partner and workforce scenarios for delegating responsibilities to speed up administration and allow administration of identities in different markets
- Global Token Processing, which ensures compliant use of services in all regions around the world and allows users to access services in all regions while the user’s data stays securely in his home region.

Deployment model

Service Layers complements the core IAM functionality with a range of technologies for delivering integrated, customized services from various IaaS (Infrastructure as a Service) providers including AWS (Amazon Web Services), Google Cloud or Microsoft Azure. Service Layers can also provide hosting services itself or can operate IAM services in managed Kubernetes data centers or OpenShift instances running on premise, depending on the requirements of an organization.

The Service Layers managed IAM service addresses common challenges, including:

- The cost, complexity and risk of rolling out a standard on-premise IAM service
- Setting up and operating IAM infrastructures in global environments
- Dealing with consumer identities and changes technology and regulatory landscape
- Migrating on premise IAM systems to a service-based model

The managed service approach run by Service Layers, with individual instances and customization per tenant within a well-defined framework, allows businesses to meet the need for customization while at the same time benefiting from a standards-based, managed infrastructure.

The Service Layer approach is also based on the configuration of systems through machine-readable definition files rather than by physical hardware configuration or interactive configuration tools. These “infrastructure as code” and “configuration as code” processes allow for rapid deployment and customization and enables fast and accurate auditing process to ensure regulatory compliance.

Unlike other IDaaS vendors' common approach, Service Layers uses dedicated instances for each customer, so no runtime components are shared across multiple customers. Thus, Service Layer can automate the infrastructure and configuration management, resulting in reduced operational cost.

Underlying architecture

Service Layers builds on a modern architecture, based on microservices and containers. Microservices allow for defining small, functional blocks with well-defined APIs and flexible reusability. Such microservices, as well as the pre-configured services of the best-of-breed applications used, are then packaged into containers, based on Kubernetes. These can be run on various types of infrastructure, including private and public cloud environments.

Operating model

Aimed at medium to large enterprises, Service Layers provides IAM deployments and operations in data centers in Europe, the US, and critically in China where special legal requirements apply. This means Service Layers can provide managed IAM services in all these regions, including customization for local privacy and security regulations as well as languages. Many companies are faced with replacing existing Access Management inventory systems for employees and partners due to compliance and security reasons. The managed IAM service from Service Layers enables companies to meet all security and

compliance requirements quickly and consistently.

Additional services

Unlike many other IDaaS providers, Service Layers ensures that IAM interfaces for products that have product lifecycles of 10 to 15 years will be supported even if the manufacturers wants to move away from the platform, because Service Layers is based on market leading products and customers own all services that form part of the implementation.

Service Layers also integrates a consistent DevOps approach, allowing for agile delivery and enhancement of the service. This includes features such as CI/CD pipelines, auto-scaling and more. Version and release management ensure code is always in a stable state and quality is assured by integrated and automated testing. This means companies can benefit from short development cycles and a shorter time to market through the fast integration of new services.

Service Layers focuses on full automation of both the delivery pipeline and operations, by making use of common, modern DevOps infrastructure components. These include Gitlab, Docker Containers, Kubernetes, and OpenShift. For capability enhancements and customizations, several additional established infrastructure components are used, including Elasticsearch and PostgreSQL.

While Service Layers provides a high degree of re-use amongst customers and thus efficient delivery, data is fully segregated, and deployment and configuration options remain flexible due to separated instances for each customer. Customers can choose the:

- Deployment model and cloud infrastructure to use
- Level and availability of support
- Degree of customization

While offering these customization options, Service Layers standardizes operations, security patch management, and other services across all customers. Furthermore, each customer instance is supported by a defined project team for both customization and operations.

iC Consult, via its Service Layers subsidiary, is one of several system integrators that have begun delivering IAM services in a managed service offering, distinguished by:

- A strong focus on optimized delivery and customizations
- An ability to balance well a standard implementation with customer-specific requirements
- A strong globalization strategy, focusing on key regions
- Focus on manufacturing companies, with strategic plans to extend coverage to a variety of target industries, including financial services.

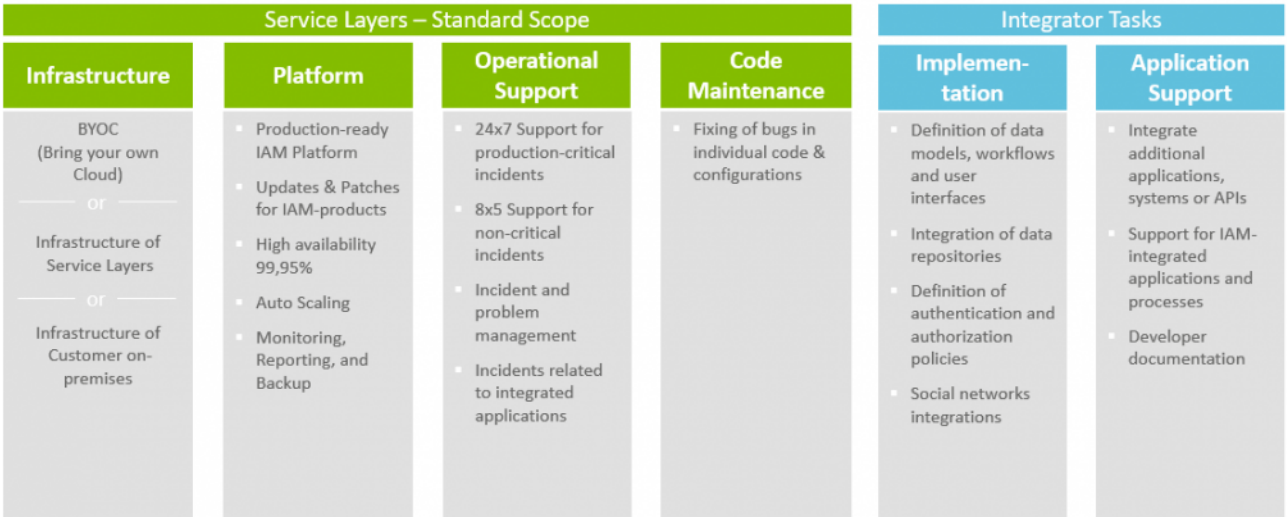

Figure 2: Building blocks of Service Layers (Source: Service Layers)

From an architectural perspective, Service Layers builds upon state-of-the-art concepts, which is the foundation of a flexible and future-proof service. And basing the offering on well-established, best-of-breed products gives customers the reassurance of building on a stable environment.

Service Layers provides an interesting option for deploying and running IAM in local or global environments for businesses of different sizes, with a well-thought-out architecture and operating model. For organizations facing the challenge of running an IAM that fits to their hybrid IT environment, especially if they need to support worldwide operations, we recommend evaluating Service Layers.

7 Recommendations

Success in providing an IAM service in a constantly changing IT, business and regulatory environment, particularly for multinational companies, lies in the ability to adapt quickly to new requirements.

Whatever approach a company decides to take, there are essential requirements that must be met when setting up an IAM in global organizations.

1. Organization
   Organization, accountability and responsibility must be well defined across the global organization.
2. Defined services
   IAM services must be well defined and comprehensive with service descriptions and SLAs.
3. Consistency and flexibility
   Consistency is key but will work only with sufficient and defined flexibility for regional/local specifics.
   Based on these requirements, it would be inadvisable for organizations to run a distributed IAM because while existing investments in regional IAM would be preserved and it might appear to be the best fit for regional specifics, distributed IAM means there are multiple IAM technologies in place and, no shared knowledge, typically resulting in varying levels of maturity for IAM implementations. Distributed IAM also often results in complex technical integrations and inconsistent processes, making it extremely challenging to meet global regulatory requirements.
   Another option would be to run IAM globally. While this would ensure a consistent IAM implementation and defined IAM services and make it easier to meet regulatory compliance at a global level, for organizations to do this themselves would require them to have own data centers and operations. It is frequently difficult to ensure proper operations across the global organization. Also, running IAM globally typically includes all the challenges of IAM implementations, with projects stalling. This all becomes even more complex and challenging when done on a global scale.
   We believe the best option is running IAM globally as a service, which provides the benefits of a global IAM without the risks associated with IAM implementations. Global IAM as a service ensures a single, modern operating model across all regions, well defined accountability and responsibility, well defined IAM services backed by SLAs, and consistency and flexibility to meet local language, process and regulatory requirements. This approach avoids all implementation challenges while addressing the key challenges of scalability, consistency, cost and regulatory compliance that typically face multinational organizations in terms of IAM.

8 Related Research

Leadership Compass: Identity as a Service (IDaaS) - IGA - 80051
Advisory Note: Future of Identity Management - 71303
Buyer's Guide: Consumer Identity and Access Management Solution – 80111
Architecture Blueprint: Hybrid Cloud Security – 72552
Advisory Note: Cloud Services and Security - 72561

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.