KuppingerCole Report

WHITEPAPER

by Martin Kuppinger | November 2019

Modern Identity Fabrics:
A Cornerstone of your Digital Strategy

Digital Transformation is ubiquitous. Creating new digital business services changes the way IAM needs to be done. Instead of managing existing applications, IAM has to provide identity services that can be consumed by digital services. Focus is shifting from modern UIs for managing existing applications to APIs that provide the identity services. Modern Identity Fabrics must serve both needs and incorporate an Identity API Platform that delivers the API-based access that is required today.

by **Martin Kuppinger**
mk@kuppingercole.com
November 2019

Commissioned by ForgeRock

Content

Table of Figures

Related Research

Leadership Compass: Identity API Platforms – 79012

Leadership Compass: Access Management and Federation - 71147

Leadership Compass: CIAM Platforms - 79059

Leadership Compass: Adaptive Authentication - 79011

Leadership Compass: Identity Provisioning - 71139

1 Introduction

Digital Transformation affects all businesses, and is fundamentally changing IT. Digital Identities are moving to the center of attention in this transformation. Without the ability to manage and conrol the access of everyone to every service, businesses will fail in their transformational initiatives.

To succeed in Digital Transformation, businesses need a strong digital identity backend that delivers all identity services required by the new digital services that are created. Such backend forms the "Identity Fabric" that provides all services in a standardized manner and, beyond that, integrates back to legacy IAM.

With Identity Fabrics, programmatic access from digital services to the Identity Fabric and its identity services becomes the norm. APIs (Application Programming Interfaces) come into play. APIs are defined interfaces that can be used to call a service and get a defined result. APIs are what is used to integrate different solutions – developers call an API, in the case of the Identity Fabric, to consume an identity service.

Identity API Platforms provide identity services via APIs. A platform as a whole should deliver a comprehensive set of services, from Directory Services to Identity Lifecycle Management, Access Management Services, and potentially even Access Governance. Even API Security and Management may be part of these services. They might be provided as an integrated solution (rarely) or a combination of several underlying technical building blocks that deliver various elements of the service.

Identity Fabrics are more than Identity API Platforms, both regarding capabilities and interfaces. However, the shift to API-based access in consequence of Digital Transformation requirements changes IAM and puts the API capabilities at the center.

A well-thought-out Identity Fabric should rely on a small number of components. This number will rarely to never be zero, given that there are no solutions that cover all aspects of IAM, not to speak of solutions that are even close to best-of-breed across the broad range of IAM capabilities.

ForgeRock counts amongst the well-established vendors in the IAM market. In contrast to most others, ForgeRock very early had a strong focus on API-based access. This distinguishes ForgeRock offerings from most other vendors in the IAM market. Many ForgeRock customers already have started building their digital services on the ForgeRock platform, which thus factually delivers the Identity API Platform that forms the core of the Identity Fabric of these customers.

We recommend organizations starting to revisit their current approaches on IAM and shifting to a multi-speed approach that serves the requirements of building new digital services in Digital Transformation immediately, while also allowing for a gradual migration and integration of legacy IAM services and existing applications.

2 Highlights

- The concept of Identity Fabrics: A logical architecture for IAM that serves both the requirements of delivering identity services to the digital business and supporting the current IT infrastructure
- Adding identity services based on APIs that can be consumed by new business applications, and ensuring that there is a comprehensive, consistent, and stable identity API layer
- The need for Identity API Platforms that deliver the APIs
- Reducing complexity of Identity Fabrics by building on a small set of core technologies that deliver the essential services within an Identity Fabric
- ForgeRock's IAM technologies as an option for creating an Identity Fabric that supports the multi-speed approach of IAM
- Actions to take for effectively moving towards an Identity Fabric that is based on a modern Identity API Platform

3 Modern Digital Identity as Business Strategy

Identity Fabrics provide a comprehensive set of IAM capabilities. They support both the management of existing applications and API-based access to identity services for newly created applications, specifically digital services created within Digital Transformation of businesses. Such services require a central identity backend to work well, instead of multiple identity silos.

In the world of Digital Transformation, experience is king. The digital trend-setters like Amazon, Apple, and Google have focused relentlessly on providing low friction digital experiences, and customers now expect this out of every business. Interestingly, experience expectations are no longer limited to consumer-facing services. Because of the pervasiveness of digital transformation in businesses, particularly IT, business workloads are shifting to the cloud and to as-a-service models. Businesses provide digital services to their customers and consumers via apps and integrate with devices and things. Business models are changing, customer relations are changing, and business partnerships are far more volatile than ever before.

Digital Identities are moving to the center of attention in the Digital Transformation. Without it, managing customers, partners, devices, or things will not work.

Digital Identities are moving to the center of attention in this transformation. Without the ability to manage and control the access of everyone to every service, businesses will fail in their transformational initiatives. Pressure on businesses concerning digital identity comes from all sides, from regulatory bodies demanding data compliance, from consumers demanding privacy, and the business case demanding smart analytics and growth. All key aspects of identity in the digital age are at risk: privacy, security, compliance, and user experience. Businesses and their leadership teams are challenged by the need for continuous innovation of both technology and business models as well as ubiquitous change in business partnerships and internal organizations.

Identity and Access Management (IAM) for the new services that rise out of Digital Transformation must become a standard capability. But adding IAM capabilities to each new service will add costs, increase their time-to-market, and will inevitably result in limited services deployed in silos. To succeed in the Digital Transformation, businesses need a strong digital identity backend that delivers all identity services required by the new digital services that are created. Such backend forms the “Identity Fabric” that provides all services in a standardized manner and integrates with legacy IAM systems. Identity Fabrics are focused on delivering a scalable, comprehensive set of identity services to developers and to the users of digital services, and form the core of modern IAM.

Factually, a good Identity Fabric should only rely on a few essential components. These core capabilities around Identity Management (Identity Lifecycle, Directories, Access Governance,…) and Access Management (Authentication, Authorization,…) should be provided by the minimum central elements possible. But despite minimization strategies, this number will rarely be zero, given that there are no solutions that cover all aspects of IAM. Additional capabilities will add to the overall number – but start with defining the core and build on strong, feature-rich solutions here.

Solutions that follow or shift towards a consistent microservices architecture, deployed in containers are a strong option for Identity Fabrics. Correctly executed, such solutions can be easily run in a variety of deployment models, from on premises to public cloud IaaS (Infrastructure as a Service). Identity Fabrics are the logical concept, the umbrella for restructuring IAM into a set of modern services and serving the demand of Digital Transformation initiatives. They are neither a single product nor a fixed technical approach.

Businesses should not wait for their legacy IAM to deliver the identity services they need in Digital Transformation. Businesses should not wait for their legacy IAM to transform into a modern Identity Fabric. And businesses cannot afford to end up with uncoordinated identity silos across their digital services. Identity Fabrics help in rapidly delivering the unified identity service backend while allowing for migration, integration, and re-use of existing legacy IAM in a phased program, without affecting the ability to deliver what is needed for success in Digital Transformation. Businesses need a multispeed IAM– the immediate support for new requirements in Digital Transformation, and the integration and gradual migration of legacy IAM into the modern Identity Fabric.

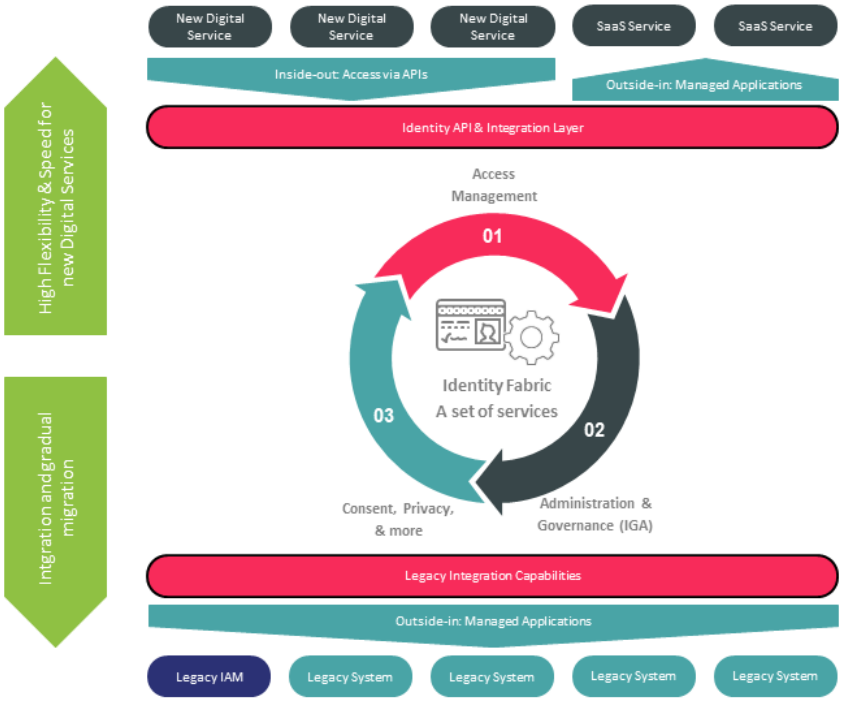

Figure 1: Identity Fabrics must support a multi-speed IAM, managing existing applications as well as providing identity services to new applications.

Forward-thinking organizations are beginning to recognize the business opportunity of taking a strategic approach to digital identity. The concept of leveraging a standardized Identity Fabric to deliver on the vast requirements of digital services has strong potential for strategic business impact. But the promise of distinguished and competitive consumer services, a more secure and streamlined workforce, and consolidated operations that reduce cost and complexity brings certain challenges. Given all the challenges facing Digital Transformation, legacy is among the greatest.

4 The Legacy Dilemma

Every organization has legacy software and systems. As organizations plan to implement new digital services, they invariably encounter the Legacy Dilemma: How do they move forward at the required pace without breaking their legacy environments? The dilemma applies equally to legacy identity management systems.

The first generation of identity management software was largely driven by enterprise compliance initiatives, which required accurate reporting about which employees had access to what systems. These systems were costly, complex to implement, and had limited scalability. A new form of identity management software emerged built mostly for consumer-facing web applications, and was largely developed in-house in response to support early waves of digital transformation. This new wave became known as "Customer Identity & Access Management," or CIAM. Finally, as API-first systems began to underpin software applications, and the Internet of Things became part of the technology lexicon, identity management for all forms of non-person entities became a reality.

Each generation of identity software was developed to meet the requirements of its time. And with each iteration, digital identity became a more central and critical business success factor. Although today's business requirements for an Identity Fabric have never been stronger, the reality is that almost every organization has pieces and parts of existing identity systems from each of the three generations. Further complicating matters, first generation identity systems are generally more proprietary than open. Second generation CIAM systems vary wildly, and struggle to keep pace with evolving experience and security requirements. Worse still, many present-day identity solutions are narrowly focused--further contributing to the legacy dilemma.

With a modern Identity Fabric, the legacy dilemma is mitigated by changing the paradigm between legacy and modern systems from an either/or to a yes/and. This embodies the multispeed system approach, which chooses a digital identity backend that adapts quickly to new digital services while gradually but deeply integrating with legacy systems to allow Digital Transformation from the core. This outcome is achievable when the Identity Fabric is built on an API-first platform that uses open standards, offers targeted legacy integration solutions, and includes extensible implementation choices, including As-a-Service, Hybrid Cloud, and On-prem software deployments.

5 Overcoming the Legacy Dilemma

The concept of using identity services from a central platform is not entirely new – it is a common element in mainframe infrastructures. APIs move to the center of attention. Identity API Platforms must deliver a comprehensive, consistent, and stable set of such APIs.

Using a multispeed approach to overcome the Legacy Dilemma requires two things of a solution: first that it has the ability to integrate with legacy systems, and second that it empowers new digital services to operate on a central identity platform. This second requirement marks the rise of a critical trend in IAM: the use of standardized APIs to deliver Identity as a Service.

Identity Fabrics establish a norm of creating programmatic access from digital services to the Identity Fabric and its identity services with APIs (Application Programming Interfaces). APIs are defined interfaces that can be used to call a service and get a defined result.

There is a fundamental difference between traditional IAM and the way API-based access works. In traditional IAM, IAM works outside-in to the application. It uses interfaces provided by the application, including standard protocols, to make changes or provides services such as authentication to the application. In digital services with API-based access, the process is inside-out where the target applications request identity services internally from the Identity Fabric.

There is a fundamental difference between traditional IAM and identity services supporting new applications: In the latter case, business services actively access identity services, instead of being passively managed.

APIs that take an active role in accessing identity services essentially provide Identity as a Service, enabling new digital services to integrate with a cohesive identity management system, such as an Identity Fabric. Many businesses are software business today, incorporating digital services into the physical goods they sell and adding further digital services to their business models. These services, from new banking and insurance services to home automation, connected vehicles, or modern machinery, are all digital services, and they all require digital identities – and they are all home-grown software. That type of software, wherever it runs – centrally, in a machine, or in an IoT device – must be able to consume the digital identity services. And it does so via APIs (Application Programming Interfaces). Essentially, this is real “identity as a service” – a service that can be consumed flexibly by all the applications.

Identity API Platforms should deliver a comprehensive set of services, from Directory Services to Identity Lifecycle Management, Access Management Services, and potentially even Access Governance. Even API Security and Management may be part of these services. They might be provided as an integrated solution (rarely) or a combination of several underlying technical building blocks that deliver various elements of the service.

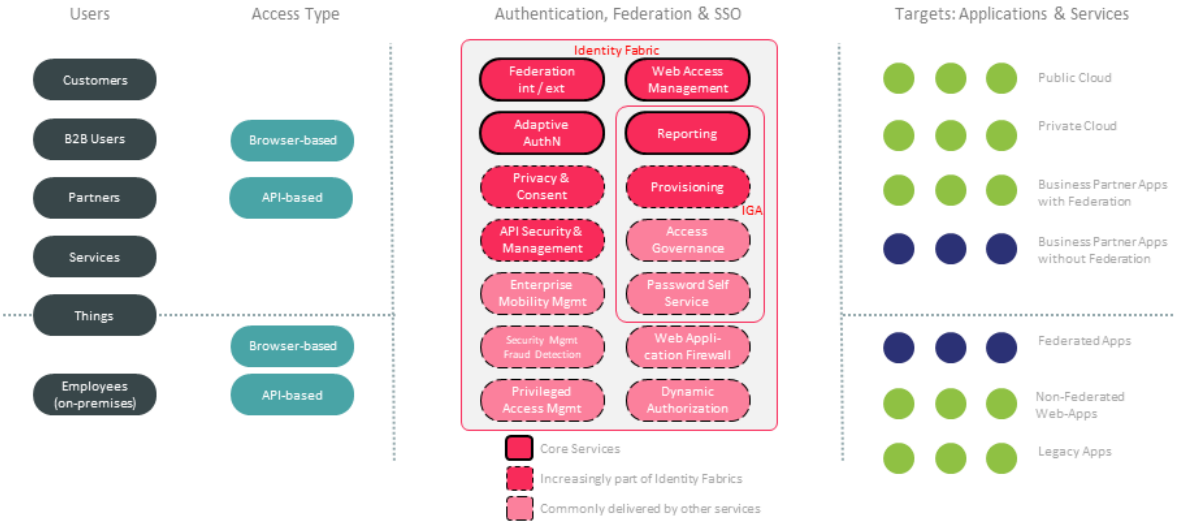

Figure 2: Identity Fabrics must incorporate an Identity API Platform and deliver a comprehensive set of identity services.

However, it is essential to have a comprehensive, stable, consistent API layer on top of the Identity API platform. Businesses should avoid lock-in to an Identity API platform when they build their digital services upon one. Long-living digital services – and some will live long – must operate on an Identity API Platform that is stable but that has the freedom to be replaced, changed, or extended if ever required.

It is essential to have a comprehensive, stable, consistent API layer on top of the Identity API platform

6 ForgeRock: Delivering the Foundation for Building Your Identity Fabric

ForgeRock is an established player in the global IAM market, with a presence in all major regions. In contrast to many of the other vendors in the IAM market, ForgeRock followed an API-first, platform-centric approach from the very beginning. ForgeRock already delivers on the promise of Identity Fabrics with their highly scalable platform for managing and governing all types of identities and their access management, including securing API-based access.

Successful Identity Fabrics must be flexible. With dynamic orchestration and intelligence capabilities at the center of their Identity Management, Governance, Access Management, Directory, and Edge Security capabilities; ForgeRock can provide the flexibility and agility required by modern businesses when building new digital services, or integrating with legacy systems. Moreover, ForgeRock can be run in both as-a-service and on-premises deployment models, and has deep support for automated DevOps deployments. Thus, ForgeRock is well-prepared for serving the requirements for a multi-speed IAM.

Beyond the common scope of humans accessing systems, ForgeRock also has a strong focus on the ever-growing world of connected things. All of their solutions allow for the integration of things, and ForgeRock even delivers a separate solution for IoT security: ForgeRock Edge Security. In Digital Transformation, connecting things is paramount for business success, both for Consumer IoT, such as smart watches, GPS devices, and all the things within connected vehicles; and for Industrial IoT (IIoT), where more and more sensors and other kinds of devices are increasingly becoming connected.

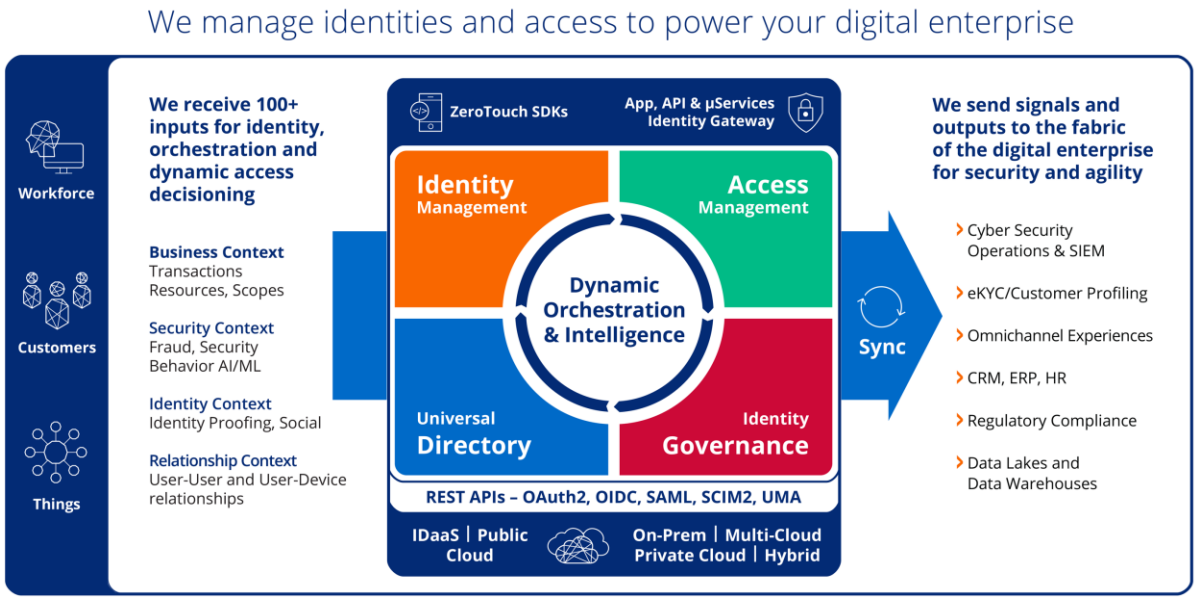

Figure 3: ForgeRock's approach on IAM focuses delivering the identity and access services for the digital enterprise (Source: ForgeRock)

The ForgeRock Identity Platform

The ForgeRock Identity Platform is an integrated set of standards-based, API-first digital identity solutions that is proven capable of serving as the basis for establishing an Identity Fabric. The platform includes identity management and governance, access management and strong authentication, identity gateway, directory services, privacy and consent with user-managed access (UMA), and edge security.

Its architecture is designed from the ground up as a unified, modular system with shared service components accessible through REST APIs and SDKs, making it easier to develop, implement and manage deployments. The platform leverages industry standard protocols, including HTTP, XML, REST, SAML 2.0, OAuth 2.0, UMA, OpenID Connect, FIDO2, and W3C Web Authn to deliver a high performance, highly scalable, and highly available IAM solution. Shared services include a Common REST API, Common UI Framework, Common Auditing and a Common API Explorer.

Functionality is decoupled so that the different components within the platform are designed for specific jobs. This decoupling of functionality, along with the standards-based interfaces, allows components to be used independently of each other and in conjunction with other technologies from other suppliers.

ForgeRock provides support for managing and governing all types of digital identities through their strong federation and standards support, backed by their own high scale Universal Directory. The later can be used for managing the identities of consumers, citizens, partners, employees, devices, and other data at scale through the use of ForgeRock Identity Management. Rich synchronization and reconciliation of identities and progressive profiling, coupled with ForgeRock Directory Services provides the identity lifecycle management needed to not just unify identities but lay the groundwork for digital services that require personalization. This is essential where the relationship of humans, devices, and things must be managed.

One of the most innovative features ForgeRock offers is its Intelligent Authentication Trees, an intuitive, flow-chart-based policy authoring tool. Authentication Trees allow customer admins to flexibly create policies in the GUI that meet the levels of assurance needed for sophisticated use cases. The details of designing complex, risk-adaptive authentication and authorization rules are abstracted by the interface. In the latest release, ForgeRock has introduced Registration Trees, which allows businesses to set up customizable registration flows, similar to Authentication Trees.

ForgeRock provides a comprehensive set of capabilities, serving the key areas of an Identity Fabric. These include

- Directory Services: the ability to link and manage the identities of everything from employees, customers, citizens, partners, devices, things, and services
- Identity Provisioning, Lifecycle Management, and Access Governance: capabilities required for setting up user accounts in target systems, including SaaS applications; this also covers Identity Relationship Management, which is essential for digital services where the relationship of humans, devices, and things
- Intelligent orchestration: configuration of identities, services, and their relationships to support varying business needs
- Multispeed IAM: giving organizations the ability to use and develop new digital services while also connecting back to legacy systems
- Flexible Deployment: deploy an identity platform in any cloud environment, on-premise, or hybrid depending on their business needs
- API Security & Management: with good baseline capabilities in managing the APIs and their security, enabling organizations with the ability to embed identity fabric functionalitz to make their applications identity aware

With this comprehensive set of capabilities, ForgeRock delivers a strong foundation for building the customer's Identity Fabric. Furthermore, as one of the established IAM vendors, ForgeRock is not only strong in supporting new digital services and SaaS applications, but also in connecting back to on premises applications and legacy. Thus, it is prepared for gradually converting legacy IAM into the newly built Identity Fabric.

7 Time to Value:Operating an Identity Fabric as a Cloud Service

Deployment models for Identity Fabrics are dependent on contextual requirements. There is no mandate for a particular deployment model, and for the most part Identity Fabrics will run on a hybrid model, combining the strengths of on-premise and cloud solutions. For years ForgeRock has been a leader in on-premise IAM solutions. In the fourth quarter of 2019, ForgeRock launched cloud IAM services: The ForgeRock Identity Cloud.

Identity Cloud Express is the SaaS version, which features pre-configured templates, developer guides, sample code, self-service registration and user management, access management, Authentication Trees, and authentication methods including the latest in passwordless and API management. Like the on-prem version, it supports the latest standards such as FIDO 2.0 WebAuthN, OAuth 2.0, and OIDC.

Identity PaaS boasts the same full feature set as their on-premise Identity Platform including: full identity lifecycle & relationship management, identity sync & provisioning, and end user self-service; adaptive & risk-based authentication including SSO and MFA; fine-grained authorization policy; universal directory; dynamic orchestration and intelligence; and privacy and consent management. This offering allows customers who want to utilize the cloud but who also need the flexibility and extensibility of Identity Platform. The primary benefits of this approach are automatic scalability and less infrastructure to manage. Customers can retain full control of their IAM solution without having to maintain the underlying hardware, operating systems, and databases.

ForgeRock Identity Cloud is able to provide the same feature set as their on-premise versions because they run the same code. Some legacy IAM vendors run different codebases between the different versions and delivery models they support. This can lead to significant differences in the capabilities and scalability between versions.

ForgeRock is positioning Identity PaaS for customers who need enterprise grade IAM functionality. Some customers report that, although they like the cloud-first approach that some IDaaS and CIAM vendors have taken, they can't get the full set of IAM features from those offerings. These customers need multiple MFA options, risk-adaptive authentication and conditional access authorization, support for high assurance credentials, and tight integration with IoT devices. ForgeRock Identity PaaS is the solution that provides advanced IAM functionality to facilitate building Identity Fabrics as a platform in the cloud.

ForgeRock Identity PaaS is also a means to help bridge the gap between legacy on-premise IAM and applications and new Digital Transformation initiatives born in the cloud. Identity PaaS can serve as the Identity Fabric that eases the transition to primarily cloud-delivered services, thereby enabling the multi-speed deployment model and architecture referenced above.

With the expanding focus of digital identity from first generation, employee-centric IAM to Identity Fabrics that support access for sometimes tens or hundreds of millions of consumers, employees, and their related things and devices, scalability becomes a far bigger issue than ever before. ForgeRock has a strong track record of delivering solutions that scale massively to meet customer needs. Overall, ForgeRock is well-positioned to act as the foundation for Identity Fabrics that enable businesses to speed up their Digital Transformation.

8 Action Plan for implementing an Identity API Platform for your Identity Fabric

Setting up an Identity Fabric required defining a comprehensive “big picture” target state that is based on a phased implementation. The latter commonly starts with delivering identity services for new applications that are created in the Digital Transformation, and subsequently migrating legacy IAM and integrating existing applications.

Business must modernize their approach on IAM to become ready for delivering the identity services that are required in Digital Transformation. It is essential to take this journey following a multi-speed approach, where the requirements in building new digital services are served rapidly, while legacy IAM continues to operate while migrating over time.

On the other hand, the concept of the Identity Fabric must be comprehensive, covering all aspects of IAM. It may start with the major services and become extended over time, but it must cover both the outside-in and inside-out approaches on IAM – managing target systems and serving the new applications that use the APIs of the Identity Fabric.

For moving to an Identity Fabric, we recommend following 10 steps:

1. Identify the state of IAM for both legacy IAM and modern IAM serving the digital services.
2. Understand the requirements for modern identity services within the Digital Transformation of your business, specifically with identities that need to be served, from employees to customers or connected things.
3. Define the main capabilities and services of your future Identity Fabric, based on these requirements and the need for gradually migrating your legacy IAM.
4. Run a gap analysis of your current state compared to the to-be-state of a modern Identity Fabric, building on an Identity API Platform.
5. Define your future Identity Fabric.
6. Select an appropriate technology or set of technologies for the core services of your Identity Fabric, and add additional capabilities and the underlying technologies wherever required. Identify where you can continue to use existing technologies and whether/when these need to be migrated.
7. Revisit the APIs provided by the technologies and define a consistent, stable API layer based on that.
8. Educate software architects and developers on how to use these APIs. Add SDKs wherever required for simplified consumption of identity services by the developers.
9. Plan for a gradual migration of your legacy IAM.
10. Start building your digital services based on your Identity Fabric.

It is essential to work closely with various teams, specifically the application architects and developers of digital services, but also the IAM team that runs the current IAM infrastructure.

9 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**

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