

# Digital Transformation for Business Enablement Requires a Modern Identity Fabric

Digital Identities are at the heart of the Digital Transformation. Without the ability to unify identities and manage the access of everyone to everything to every digital service effectively, transformation initiatives will fail. Business can't afford to implement these capabilities on a per service basis – this will increase cost, slow down time-to-market and lead to new identity silos, resulting in a negative user experience. By setting up an Identity Fabric that delivers identity services to the new digital business services, organizations can meet the demand of Digital Transformation initiatives quickly, while enabling a gradual migration of their legacy IAM.



by **Martin Kuppinger**  
[mk@kuppingercole.com](mailto:mk@kuppingercole.com)  
November 2019

Commissioned by **ForgeRock**

## Content

<b>1 Introduction .....</b>	<b>3</b>
<b>2 Highlights .....</b>	<b>4</b>
<b>3 Identity at the Heart of Digital Transformation .....</b>	<b>5</b>
<b>4 Identity should not be an obstacle to innovation – get rid of identity silos .....</b>	<b>7</b>
<b>5 Identity Fabrics: The new, central IAM layer .....</b>	<b>10</b>
<b>6 Action Plan for implementing an Identity Fabric for fostering Digital Transformation .....</b>	<b>12</b>
<b>7 Copyright .....</b>	<b>13</b>

## Table of Figures

Figure 1: Identity Fabrics enable businesses to rapidly deliver new digital services, while gradually integrating with the legacy IAM. ....	8
Figure 2: Identity Fabrics deliver a broad range of IAM services and enable flexible access to all types of applications. ....	10

## 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 Digital Transformation is changing IT in businesses fundamentally. 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 this transformation. Without the ability to unify identities and control the access of everyone to every service, businesses will fail in their transformational initiatives. No business is unaffected by the Digital Transformation. 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.

There are many things business leaders need to do for their businesses, not only to survive, but to excel in Digital Transformation. One of the essential imperatives is putting Digital Identity at the center. In an age where direct services to consumers are the norm, where relationships to these consumers remain key to success but are under permanent threat, where business relationships change faster than ever before, and where all services become digital, identity is what links everyone and everything: employees, customers and consumers, business partners, but also their devices, things, and services. Identity is at the heart of true Digital Transformation.

Enabling access of employees to new cloud services and evolving the employee experience in using digital services is essential, as it is to enable seamless, yet secure access for potentially tens or hundreds of millions customers and consumers to new digital services. Digital leaders must balance their transformation efforts for enabling both the transition into a digital organization and the evolution towards digital business.

IAM for the new digital services must become a standard capability. Managing customer identities at various places will lead to disruption and a negative user experience (UX) for the customers. Adding IAM capabilities to each and every service will add cost to developing such services, increase their time-to-market, and will inevitably result in limited services deployed in silos.

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. 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.

Businesses can’t wait for their legacy IAM to deliver the identity services they need in Digital Transformation. Businesses can’t wait for their legacy IAM to transform into a modern Identity Fabric. And businesses can’t afford ending 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.

ForgeRock is an established player in the IAM market, delivering the elements required for setting up such an Identity Fabric. With strong API support, high scalability and the ability to manage all types of identities, including devices and things (based on specific IoT support), ForgeRock can provide the layer that businesses need for speeding up their Digital Transformation: An Identity Fabric.

## 2 Highlights

- The need for Digital Identities in Digital Transformation
- Changing perspectives on identities: Beyond employees, managing identities of consumers, customers, business partners, but also devices, things and services
- Avoiding new silos: The need for an identity backbone – the “Identity Fabric”
- Enabling bimodal IAM: Identity Fabrics serving new digital services and connecting back to legacy IAM
- Architecting an Identity Fabric: Focus on the key capabilities required for new digital services
- Recommendations for implementing an Identity Fabric

### 3 Identity at the Heart of Digital Transformation

*Digital services are about connecting customers and consumers with the business. Managing their identities and access to these services is an essential capability within each and every Digital Transformation initiative.*

The Digital Transformation concept started many years ago, although in certain industries such as retail, it is still far from an end-state. Many industries, from automotive to finance or utilities, are still in the early stages of their transformation. While Digital Transformation is frequently perceived as being consumer-centric, reality shows that it affects virtually every business. B2B relationships are changing, as are employee work habits in modern, digital organizations. Digital Transformation is ubiquitous.

Business relationships are changing, with intermediaries being replaced by new services. One such example is the insurance industry, where brokers are challenged by the changes brought on in the online insurance business. Other businesses that had only a B2B market strategy before are now starting to sell directly to consumers. In B2B relations, services for control and maintenance of production equipment, for example, add to the original product's sales process and revenue. Cars are increasingly used in pay-per-use models as a service, instead of buying the product. Banks are under pressure from new market entrants who are forcing them to adapt to the challenge of maintaining customer relations without a costly customer-facing front end. Thus they risk losing their position as being the face to the customer.

---

*No business is left unchanged by Digital Transformation. Being strong in managing digital identities is a key success factor in that change.*

---

No business is unaffected by the Digital Transformation. 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.

There are many things business leaders need to do for their businesses, not only to survive, but to excel in Digital Transformation. One of the essential imperatives is putting Digital Identity at the center. In an age where direct services to consumers are the norm, where relationships to these consumers remain key to success but are under permanent threat, where business relationships change faster than ever before, and where all services are becoming digital. Identity is what links everyone and everything: employees, customers and consumers, business partners, but also their devices, things, and services.

Without well-managed digital identities, revenue will be lost, brand reputation will suffer, and business partners will not succeed in working on joint initiatives. Without getting a grip on digital identities, many initiatives in Digital Transformation will simply fail.

---

*Consumers, customers, business partners, and employees all expect great user experiences, and well-managed digital identities are the foundation.*

---

Charging customers for services requires digital identities. Secure access requires information about who is using which devices. Linking information requires an understanding of who owns which devices and things.

Consumers, customers, business partners, and employees all expect great user experiences. These stakeholders are inextricably linked together in forming the foundation of any business, and increasingly the experiences created for one stakeholder must be supported by the experiences of another. Their loyalty and commitment are shaped by experience of interactions when using new digital services. Such experience is sometimes even more complex to implement, when transforming traditional services into new online applications and services. Without understanding who is using the services, how he or she is using the services, and what he or she expects, it is impossible to deliver services that are targeted to the individual. Failure to manage digital identities well, threatens entire Digital Transformation initiatives.

## 4 Identity should not be an obstacle to innovation – get rid of identity silos

*Digital Identities must not be managed individually per digital service. This will increase cost, slow down time-to-market, and frustrate users with an inconsistent user experience. Don't create new identity silos for digital services, but build on a strong identity backbone – the Identity Fabric.*

Bringing in an identity point solution for a specific service is not the solution. It may result in one good service, but what about the next service? Businesses need to consider how to converge existing services into new ones, with more capabilities, improved business models, and an innovative user experience, while providing room for extensibility in the future.

IT is traditionally organized in silos. Unfortunately, these silos don't go away with Digital Transformation. In many businesses, Digital Transformation adds new silos because various line-of-business departments and segregated units all work as "Digital Factories" to deliver new digital services. However, they all serve the same people.

Ideally, traditional IT should be able to deliver identity services that all these initiatives could build upon. Unfortunately, IAM of today's businesses is still primarily targeted on employees, frequently still lacking coordinated approaches on dealing with other identities such as customers and consumers, not to mention non-human identities for devices and things, and their relationship to the human identities.

---

*Many organizations today operate a wild mix of different IAM tools. Moving towards an Identity Fabric helps in homogenizing IAM services.*

---

Beyond that, many organizations today operate a wild mix of legacy, home-grown, point solutions and some standard IAM products to secure and manage the identities of users and their access to current systems, applications, and services. Many organizations even lack central capabilities such as defined and consistently-enforced access policies or the ability to manage access to all the upcoming cloud services in an integrated approach to the existing on premises applications and services.

New requirements, such as managing identities and access for new groups of users that are essential to Digital Transformation, remain unfulfilled – IT just can't deliver on time. If it takes too long to provide the digital identity services for a new digital service, these digital services will not wait but figure out their own, proprietary solution. Unfortunately, such per-service solutions are just another silo.

All too often, IAM is the biggest challenge in delivering new digital services. Integrating identity with existing services typically takes too long and commonly results in fragile, individual integrations – if it happens at all. IAM today also often adds complexity to Digital Transformation, instead of fostering innovation. It is an Innovation Gatekeeper, instead of making innovation happen faster.

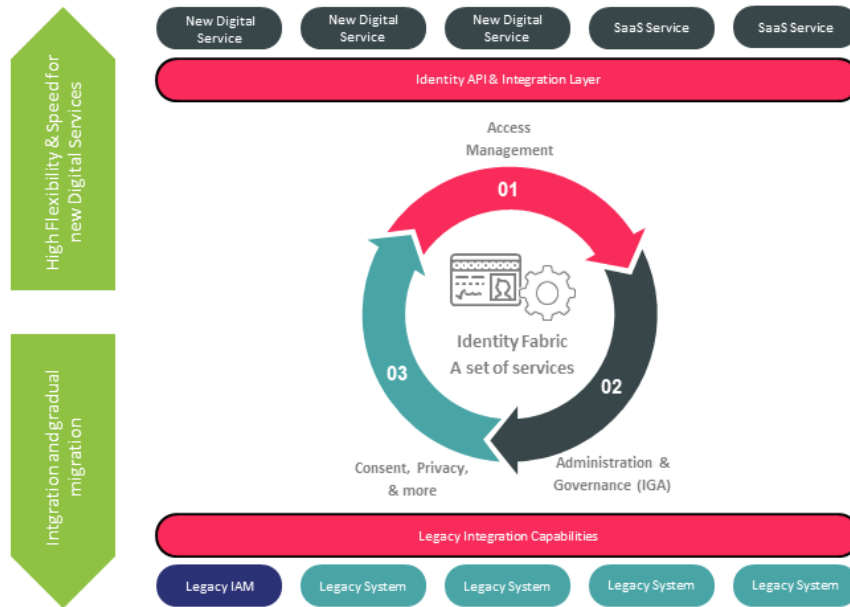


Figure 1: Identity Fabrics enable businesses to rapidly deliver new digital services, while gradually integrating with the legacy IAM.

Businesses need to rethink their overall identity strategy. While it is impossible to rearchitect and rebuild the existing IAM infrastructure in time, it is straightforward to take a multi-speed approach to IAM, resulting in a bi-modal IAM during innovation and migration of all IAM. Such a multi-speed approach starts with a unified platform for delivering Identity Services required by the Digital Transformation initiatives. That platform enables unifying all identities across all the digital services, avoiding a new set of silos. It also acts as the integration and migration target of existing IAM services over time, without negatively impacting the rapid delivery of identity services to the digital business.

---

*An Identity Fabric enables unifying all identities across all the digital services, avoiding a new set of silos and also acts as the integration and migration target of existing IAM services.*

---

This platforms then becomes the Identity Fabric for Digital Transformation. They provide the set of services that are required for managing all the various identities and their relationships.



In contrast to most legacy IAM services, Identity Fabrics are not focused on the graphical user interfaces, but on delivering the APIs and the toolsets that are required by the developers of the digital services.

Businesses can't wait for their legacy IAM to deliver the identity services they need for Digital Transformation. Businesses can't wait for their legacy IAM to transform into a modern Identity Fabric. And businesses can't afford ending 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 the Digital Transformation.

Organizations need to reconsider IAM as a whole and transform it step by step into a set of discrete but integrated and scalable services that allow consumers, B2B customers, contractors, and employees to have the appropriate level of access and usability to drive business forward in the era of Digital Transformation.

## 5 Identity Fabrics: The new, central IAM layer

*Identity Fabrics are a logical architecture that commonly builds on multiple tools. They are flexible in deployment and operating models. They excel in supporting API-based access, beyond traditional UI-based IAM capabilities.*

Identity Fabrics have a dual function. On one hand, they are the single, integrated, and highly scalable IAM platform for the emerging digital services that businesses create as part of their Digital Transformation initiatives. On the other hand, they connect back to existing IAM and thus deliver controlled access to legacy IT systems, building a bridge to these and allowing for gradual migration of existing legacy IAM capabilities. Identity Fabrics support new services while not requiring businesses to renovate their entire IAM immediately, which would be unrealistic. While legacy IAM will continue to serve the regulatory compliance requirements of employee IAM during this transition phase, Identity Fabrics are about business enablement: They help businesses to implement their new digital services faster, more securely and more efficiently. They enable businesses to be on time in Digital Transformation.

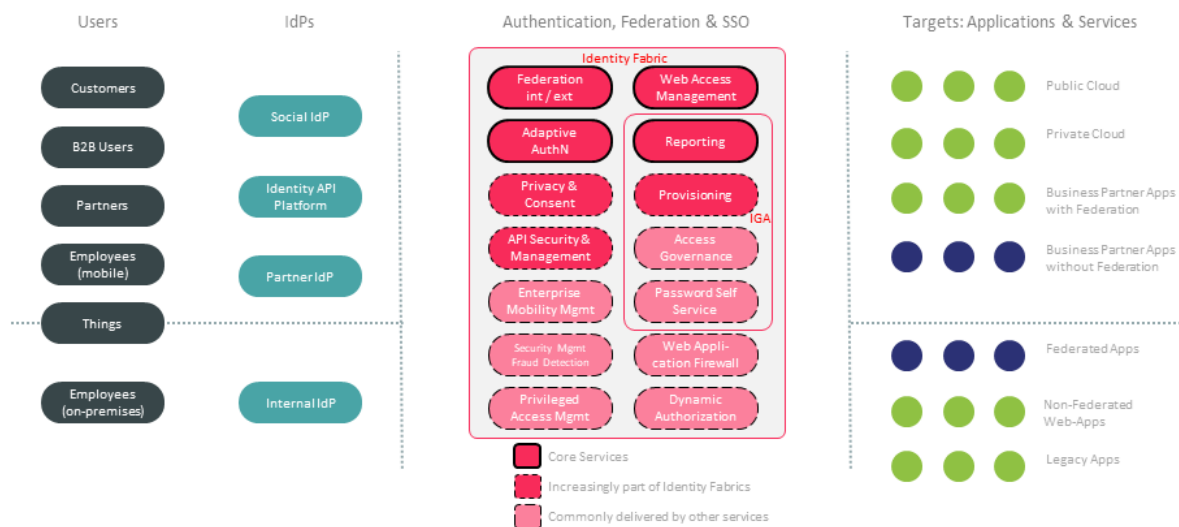


Figure 2: Identity Fabrics deliver a broad range of IAM services and enable flexible access to all types of applications.

Identity Fabrics first of all are a concept, not a single tool – as it is the case with other fundamental concepts in modern IT such as Cloud Computing or Zero Trust. When defining your Identity Fabric of the future, start with the core capabilities that are required for the quintessence of IAM: Connecting every user to every service.

Identity Fabrics, thus, are centered around managing all types of identities in a consistent manner, and around managing access to services. They must support both their own directory services and, even more importantly, support federating external identities from other identity providers. Enabling access in a controlled manner builds on adaptive authentication capabilities and outbound federation support to a variety of services, which in the Digital Age are specifically modern services supporting today's open standards such as OAuth 2.0 and OpenID Connect. New digital services can build on the services of the Identity Fabric and rely on their capabilities for managing identities and access. Done right, an Identity Fabric can rapidly deliver the capabilities for enabling access of all the various users in the digital business.

---

*The mandate to IAM is simple: Connect everyone (and everything) to every service.  
That is at the core of what an Identity Fabric must deliver.*

---

Access Management for an Identity Fabric is not limited to access of humans via their browser. Increasingly, access is via apps on mobile devices and from things (consumer electronics) that are owned by the individuals. Identity Fabrics must deliver strong support for API-based access, as well as the ability for managing relations between individuals and their devices and things.

Around these key capabilities, other capabilities can be added, covering the entire breadth of IAM. Since an Identity Fabric is a set of services delivering the capabilities required for IAM in modern businesses, such an Identity Fabric can grow and add capabilities, specifically when gradually migrating legacy IAM to a modern platform.

Identity Fabrics must support both Access Management and Identity Lifecycle Management & Access Governance (or IGA - Identity Governance and Administration) use cases. They must provide the capabilities for enabling and controlling access of all users to all types of services. They must support Identity Lifecycle Management across all types of services. They must manage the relationships between organizations, people, devices, things, and services. They must provide control about all entitlements and access. These core services can be extended by other identity and security services, for providing a comprehensive set of identity services via a central Identity Platform.

Identity Fabrics should be flexible regarding their deployment and target operating model. Within the logical architecture of such platform, instances of services might even run in parallel in different environments to optimize performance and scalability or to address security concerns. This also allows for more flexibility in serving the need for a multi-speed approach in delivering identity services for the Digital Transformation and, in parallel, gradually modernizing the existing legacy IAM infrastructure.

Identity Fabrics combine the IAM services into a single identity backbone for digital initiatives across the entire organization. Digital services can rely on this backbone from the start, delivering consistent and high-quality IAM services. It is the cornerstone of the future IAM of modern, digital businesses and the target platform for modernizing legacy IAM at the pace and financial capabilities of the business.

## 6 Action Plan for implementing an Identity Fabric for fostering Digital Transformation

*Implementing an Identity Fabric is about finding the balance between rapid delivery of IAM capabilities to new digital services and integrating with legacy IAM and IT on which many businesses currently operate. Understanding the Identity Fabric as both a rapid solution for new challenges in the Digital Transformation and a target state for a gradual modernization of legacy IAM, helps in defining the roadmap for such an Identity Fabric.*

We strongly recommend evaluating the concept of Identity Fabrics for both supporting Digital Transformation initiatives and for the modernization of legacy IAM. IAM must become a service that is easy to consume and is flexible in supporting emerging business requirements.

The essential steps on the way to an Identity Fabric are:

1. Win sponsorship of both the stakeholders of Digital Transformation (i.e. the business) and of IAM.
2. Evaluate the concept of Identity Fabrics as the logical architecture that unites various services and delivers the capabilities required by the business.
3. Define and prioritize capabilities of your future Identity Fabric, specifically focusing on the need for accommodating new kinds of users and their devices and things in accessing new digital services.
4. Focus on rapid implementation of the missing but required capabilities. This is often the cause of hindrances to digital initiatives which can prevent businesses from succeeding on time and within budget. Typically this is the capability of managing access of everyone to every service, which goes well beyond just employee access.
5. Define your modernization and transformation strategy for your legacy IAM.
6. Clearly define which services will be supported by the Identity Fabric and when, and how migration of existing services will happen.
7. Educate everyone involved in Digital Transformation initiatives about the capabilities of your Identity Fabric.
8. Educate your IAM team and motivate them to make the gradual shift to the new Identity Fabric, supporting all identities and access.

Traditional, employee-centric IAM is no longer enough for fulfilling the business demands. It is time to shift focus from an IAM for running the business to an IAM that supports the change of business.

## 7 Copyright

© 2019 Kuppinger Cole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

## 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](mailto:clients@kuppingercole.com)