KuppingerCole Report

WHITEPAPER

By Anne Bailey

February 08, 2022

# Serving the Customer in the Digital Age

In an era of digital services, business will require a new approach to serving customers. Identities, particularly customer identities, are a key enabler of the transformation that is necessary to delight customers beyond superficial levels. Concepts such as the Identity Fabric can support an intentional shift towards flexible and agile consumer identity and access management (CIAM) implementations.

By **Anne Bailey**
aba@kuppingercole.com

# Content

**Commissioned by STRIVACITY**

# 1 Introduction

Organizations are under pressure to respond to the fundamental changes to "business as usual". Especially in consumer-facing industries, delighting customers given expectations of flawless user experience, security, and flexibility can be a challenging requirement to fulfil. Digital transformation itself is not the answer, but leveraging its critical enablers such as identity - particularly consumer identity and access management (CIAM) - can be a disruptive catalyst for meeting consumer needs with excellence.

CIAM solutions target and cater to the specific requirements that organizations have for interacting with and delighting their consumers. This can be in contrast to other market segments addressing identity, such as identity and access management (IAM) and privileged access management (PAM). Given that consumers may be accessing an organization's resources with identities from various providers and of varying assurance levels, the high volumes of transactions to be handled, the numerous channels that could be used, high flexibility is an absolute must in CIAM solutions.

Flexibility is an overarching theme for CIAM use cases, since implementations must often join several digital services and components to create a functioning whole. We recommend designing this flexibility in an intentional way so that organizations do not face significant challenges in managing their home-grown code. This can ensure that interoperability is maintained between components, and that end users are indeed able to access the services they need. Especially when providing digital services, the consumer should be at the center of attention.

A concept that can help propel organizations to this point is called an Identity Fabric, a paradigm that focuses on an integrated set of services, serving all types of identities and their access to any type of service. This is a capability-based view of IAM and CIAM, and gives organizations the perspective required to intentionally design flexibility into their consumer identity management.

Given that flexibility is at the forefront of a disruptive CIAM solution, Strivacity is a vendor that holds promise for a strong Identity Fabric implementation. It is a built-for-CIAM solution that delivers a comprehensive and adaptive set of capabilities. Its strengths lie in its administrative ease-of-use, an isolation-by-design approach, a modern microservices model, and inclusion of privacy and consent modules. Strivacity offers compelling options to serve customers in the digital age with excellence.

# 2 Highlights

- Understand how identity is an enabler of digital transformation
- Discuss the importance of CIAM to the digital customer experience
- Distinguish between requirements of CIAM compared to IAM and PAM
- Consider methods such as deconstructing the user journey to introduce flexibility into user experiences
- Introduce the Identity Fabric as a helpful concept to guide CIAM architectures
- View Strivacity as a possible Identity Fabric component for CIAM capabilities

# 3 A Differentiated Digital Transformation

*Organizations seeking to delight their customers should consider CIAM solutions, since identity is a critical enabler of digital transformation.*

In light of the fundamental changes to "business as usual", digital transformation has become a business imperative. External factors like ubiquitous connectivity and a wave of new business models upend the competitive landscape, and technological developments accelerate these changes. Therefore, businesses are seeking out what *enables* a digital transformation. This goes beyond choosing to adopt new technologies to understanding why expectations have changed, and to what.

In the consumer-facing world, digital transformation often must center around delighting the customer. Delighting the customer requires more than an overhaul of the customer experience. A digital transformation journey, as depicted in the figure below, could begin with reassessing the business model, products and/or services, and how to strategically compete. But the differentiating factors lie in establishing digital services: the excellence with which these services are delivered, and the robustness and ease of use with which these services are protected. These deeper changes, sometimes founded in software investment, lead to the digital experience that consumers are looking for.

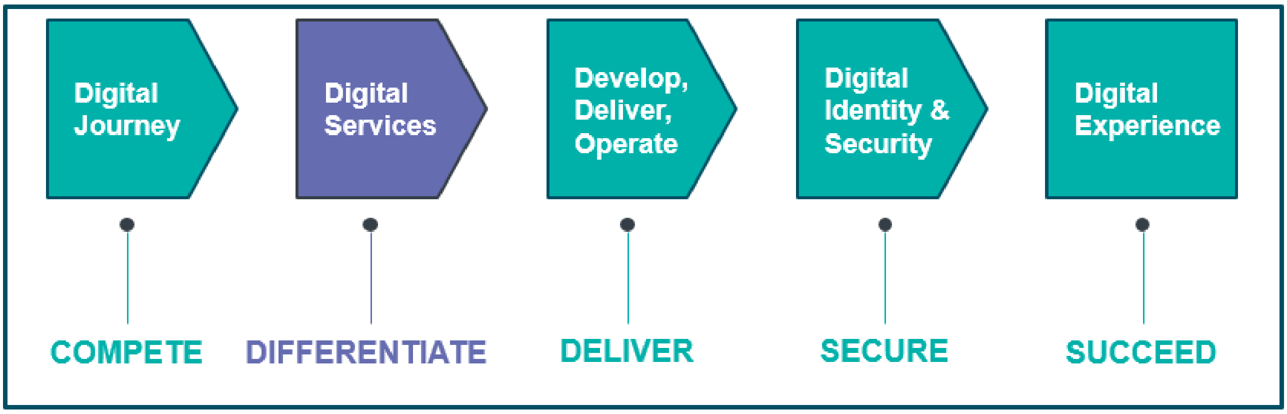

Figure 1: Steps towards creating a digital business, where differentiation often comes from digital services

If we consider these "deeper changes" that provide an excellent experience beyond the superficial level, then digital identity should be among the first topics to be discussed. Identity is a critical enabler of digital transformation, not only of security as seen in the figure above, but as a foundation for seamless digital service delivery. It facilitates and serves the hyperconnected business and its employees, partners, customers, consumers, devices, and things. It is a unifying factor by making communication and collaboration between all parties possible in increasingly interoperable ways. This heightened flexibility, new channels of communication, and secure exchange of digital identities is foundational to a digital business.

Nothing is more central to the digital consumer experience than consumer identity and access management (CIAM). On a practical level, it makes a digital user experience possible by connecting customers to the services they access. However, when delighting the customer is the goal, the deeper changes that identity makes possible can be leveraged. The customer-organization relationship is built on a balance between security and user experience with an emphasis on flexibility, and a CIAM solution should make this possible.

# 4 Differentiators of a Built-for-CIAM Solution

*CIAM is distinct from the related market segments of IAM and PAM. Notably it strives to provide external customers with the appropriate access to an organization's services. Given the diversity of profiles, assurance levels, contexts, and more that consumers bring to an organization's environment, built-for-purpose CIAM solutions can specifically meet these requirements.*

CIAM is an offshoot of identity and access management (IAM), which traditionally manages an organization's internal identity requirements. As more and more businesses developed closer and more digital relationships with their customers, CIAM emerged to meet the evolving business requirements of managing external customer access to accounts. It is now established as a market segment independent from IAM, given that the requirements organizations have of both IAM and CIAM are fundamentally different.

IAM most typically handles the identities of employees: it is focused on internal processes of provisioning, authentication, authorization, and handling changes along the employee lifecycle. Because the capabilities center on the workforce, classic IAM systems do not always have the capacity to handle the input of varied attributes for marketing and consumer management as can be provided by CIAM.

Privileged identity management (PAM) straddles the line between handling internal and external identities. It offers additional control for users that require widespread access to organizational resources, or access to sensitive resources. These are often internal stakeholders, but also can include external stakeholders like strategic partners. PAM solutions must have capabilities that allow access to the right resources by the right person at the right time.

CIAM deals with customer identities, which are external. These external identities interact with a company with a specific goal in mind: accessing a service. To achieve those goals, they only require restricted options and minimal access to organizational resources, but require access to customer portals and outward-facing resources. There is a strong shift towards flexible and strong authentication to enable the variety of consumers to access in convenient and secure ways. Here the ability to support registration and authentication with federation, particularly with social networks is key. More important than the level of assurance on those incoming consumer identities is simply the fact that they will not be lost during the onboarding process. A weak identity for a new customer is better than no new customer at all, which can be uplifted with identity vetting or verification at a later stage, for example before a purchase or other high-value transaction. Privacy and consent management is essential for consumer identities, and an area that barely impacts IAM and PAM solutions. Global regulations including GDPR regulate how the personal information of consumers may be collected and processed, which require CIAM solutions to integrate with or contain consent management capabilities. CIAM use cases do not require the fine-grained authorization capabilities that IAM and PAM use cases do. IAM and PAM solutions address the varying levels of access that employees and privileged users need to enterprise resources, but consumers rarely need access to anything more than a customer portal, meaning that CIAM solutions don't often need to include advanced authorization capabilities. These are some of the many areas where CIAM stands apart from IAM and PAM solutions.

Looking at CIAM from the organization's perspective, businesses also have specific goals in mind: to enable good customer experience, collect information about the customer to provide better services and to build more extensive profiles associated with the customer identity. It is in the interest of both parties - organizations and customers - that customers exchange information and build relationship so that each party may achieve their goal. Distinct from IAM, CIAM solutions should strive to facilitate this consensual exchange of information from consumer to organization to deliver the services that consumers expect. These goals, at times distinct from those of IAM and PAM, mean that built-to-purpose CIAM solutions will sometimes take different approaches than traditional IAM solutions to achieve them.

# 5 CIAM Requires Flexibility

*Solutions that are built specifically for CIAM use cases sometimes have distinct capabilities from other identity management solutions. But the overarching theme of flexibility depends on implementation, sometimes of different components to create a functioning whole. This concept - called an Identity Fabric - can help in designing agile and flexible identity management in the organization.*

Given the different goals that IAM and CIAM solutions must achieve, a solution that is purpose-built for customer identities and their particular use cases is sometimes a better match than an IAM solution with extended CIAM capabilities. As always, organizations seeking to find a CIAM solution should first determine their requirements, and select the solution that best fits their own requirements. But at a high level, a built-for-CIAM solution can bring advantages like policy-based configurations, synchronized databases and services, and scalability.

CIAM solutions that take a policy-based configuration approach rather than a code-based approach can keep their customers' experience always in focus. Instead of concentrating energy and resources on developers to configure the solution -- which would naturally reflect the priorities and requirements of developers and security teams -- delighting customers can sometimes be deemphasized unintentionally. Policy-based configurations put the user experience in the hands of those who know the customer best, enabling them to design branding policies, consent policies, and more. CIAM solutions that accomplish configuration in clicks not code can give a competitive edge in creating intuitive and customer-focused processes.

An API-first strategy can yield the benefits of synchronized databases and services. A CIAM solution with an API-connected identity store can keep the organization's CRM, MarTech tools, and vital Line-of-Business application synchronized and up to date. These updates are triggered by customer action and pushed automatically to the related applications.

Since CIAM solutions must handle high volumes of consumer identities and transactions, the scalability offered by built-for-CIAM solutions can be advantageous. Emphasis put on availability for all consumers anytime anywhere is sometimes shown in providing multi-instance and microservices-based deployments rather than multi-tenant options. Serving consumers means processing personal data with respect to global privacy regulations, so the ability to deploy anywhere can ensure the appropriate data residency during processing.

Flexibility remains a theme of these differentiators of built-for-CIAM solutions: flexibility to configure intuitive user experiences, to move past ridged databases that may contain conflicting information to flexible and synchronizing systems, and scalability that matches the user base. KuppingerCole summarizes this flexibility with a concept called the Identity Fabric: enabling any user to access any service, anytime, anywhere. A well-designed Identity Fabric that is founded on a standards-first framework weaves together the diverse identity types, systems, services, and devices for secure and flexible identity management.

The Identity Fabric enables identity and applications to be separated so that the IT architecture can be more agile. An Identity Fabric is a concept, not a product; it describes a set of connecting IT components that work together as a single entity rather than a concrete tool. Some principles that make up an Identity Fabric include being standards-based, leveraging microservices, being modular, enabling multi-speed functionality to legacy applications and new services, and connecting everyone to everything, everywhere at any time. The implementing organization should have well defined requirements, defined ownership and responsibility, pay close attention to interoperability and scalability while reducing engineering and time to deployment.

As organizations grow and mature, they may move from a home-grown solution to integrating different solutions into a hopefully cohesive CIAM solution. Successful Identity Fabrics typically need clear strategic priorities so that independent components and products work together as a cohesive unit to achieve the organization's unique needs. This ability to be "multi-speed", of managing access to both legacy applications and new services seamlessly, does require specific attention so that the organization is not left unintentionally being too reliant on a single protocol or standard, of not using skills and knowledge effectively, of struggling to scale, and of getting lost in multiple points of failure. These challenges of moving to a modern CIAM implementation can limit the effectiveness and the end user experience, which is why remaining focused on unique goals and requirements of the organization's CIAM solution is so important. Failing to prioritize the needs of consumers and the capabilities required to deliver services well may lead to long identity management projects that in the end don't delight consumers.

# 6 Strivacity

*Strivacity is a built-for-CIAM product delivering a comprehensive and flexible set of capabilities, including an isolation-by-design approach.*

Strivacity offers a CIAM product that is built-to-purpose and prioritizes flexibility in deployment and integration. Founded in 2019 and headquartered in Virginia, offers a comprehensive CIAM solution.

Strivacity provides an identity store, which is extensible to include the various attributes that may be required by the organization's use case. Incoming consumer data that comes from varying identity providers such as social networks, Apple, GitHub, Google, Microsoft, and others are normalized for consistent use across the organization. The identity store connects with and synchronizes other connected systems with REST APIs, supported by their proprietary Lifecycle Event Hooks. The platform allows for the creation and management of directories and databases. Strong authentication can be enabled using email, phone, SMS OTP, or Google authenticator. White-labeling of login and consumer dashboards is available.

Strivacity enables customer self-service including registration, account recovery, and account management. The registration process can be customized with no code from pre-built pages. Types of attributes to be collected from consumers are selected by the implementing organization, as well as the necessary authentication level, notification policies, and SMS/email verification. Accounts can be created manually by HR or help desks, with bulk import over APIs. Registration from networks including Apple, Facebook, GitHub, Google, Microsoft, and Twitter is supported, and provisioning from other identity providers can be configured. ID proofing can be added to the registration process to achieve higher levels of assurance. Progressive profiling is supported.

Strivacity also enables protection against stolen credentials by consuming and curating sources of compromised credential intelligence into its built-in risk engine.

Account recovery is also a self-service function, with the ability to reset password, be reminded of a username, verify with SMS or email, and be informed of other suspicious activity on their accounts via SMS/email. Self-service account management supports selecting and enrolling MFA for the first time or later when updating a device (new or stolen). imports IP reputation information and gets botnet detection capabilities from a combination of open source and commercial services. Additional intelligence services can be consumed if configured by customers. The built-in risk engine can also detect the use of new devices, take action based on activity from anonymous proxies/Tor, certain geo-graphic locations and IP ranges, and impossible travel events by consumers.

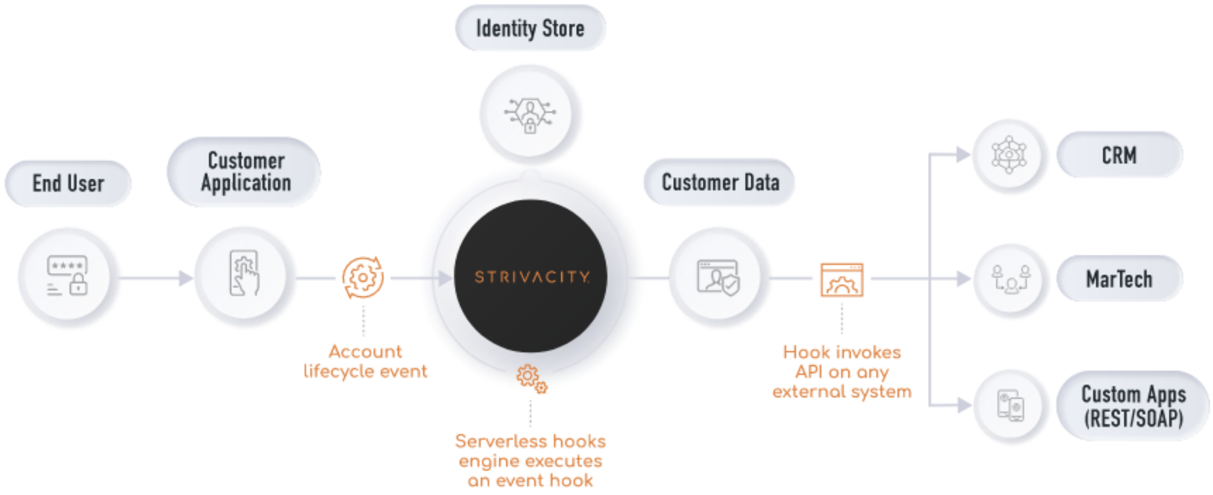

Figure 2: Architecture Diagram of Lifecycle Event Hooks, one part of the Solution, provided by Strivacity

Strivacity supports consent management initiatives by interoperating with major CMPs, CRMs, and other privacy solutions. The Lifecycle Event Hooks are key here in keeping customer databases in sync through triggering data exports, imports, and updates based on customer actions.

Strivacity is hosted in AWS and takes a serverless approach, making it easier to integrate with other systems and orchestrate the business logic already used by the implementing organization. It offers a multi-instance rather than multi-tenant approach. The solution supports OAuth, OIDC, SAML for federation and SSO with other web properties. Customers are provided separate identity data stores to ensure a high level of data separation between customers.

Overall, provides simple administrative use with high flexibility and configurability for typical CIAM capabilities. Notable are its isolation-by-design approach to providing separate SaaS instances and identity stores per customer, its microservices architecture, and its low/no code configuration.

# 7 Recommendations

Addressing your organization's need for CIAM is best done in a modern and business-oriented way. Following the Identity Fabric concept, intentionally building flexibility and interoperability between components is the recipe for providing access to any user anytime and anywhere. The following recommendations point out some suggested next steps in adopting an Identity Fabric approach:

1. **Define and verify your organization's requirements.** A successful project begins with strong and validated groundwork. Strive to understand the requirements of your business and to define those in measurable terms.
2. **Adapt a concept and architecture.** Bring these defined requirements to a concept, such as the Identity Fabric, to design your logical architecture that unites different services and delivers the capabilities required by your enterprise. Identify which services are already implemented and where they are deployed.
3. **Implement an identity services layer and digital services architecture**. Work with the teams creating digital services used by your consumers to define and implement a consistent layer of identity services and their consumption by digital services. This consistency and flexibility is an important element to delighting your consumers.
4. **Define the services and tooling.** Define the underlying technology, based on core elements and complemented by other services whenever required. Also define whether and how existing elements of CIAM are incorporated and/or gradually replaced.
5. **Identify the appropriate deployment model:** Ensure that the solution, tooling, and approach support your requirements, specifically the elasticity and scale required for supporting digital services.

Based on these steps, organizations can make a huge step forward in delivering the digital services and experience expected by consumers, by managing the digital identities of humans, devices, and things well.

# 8 Related Research

[Executive View: Strivacity Fusion - 80544](#)
[Leadership Compass: Identity Fabrics - 80514](#)
[Leadership Brief: Leveraging Identity Fabrics on Your Way Towards Cloud-Based IAM - 80501](#)

# Content of Figures

# Copyright

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.

**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.