ForgeRock

CIAM

How to Compare Digital Identity Management Providers for CIAM Within the Retail Industry

A Workbook

The retail landscape continues to shift dramatically. Retailers are ricocheting from increased (and often unmet) consumer expectations to pursuing automated, brand-driven personalization activities alongside a deepening void between digital and physical shopping channels. Against an unrelenting backdrop of increased data breaches, identity theft, and inappropriate use of personal data, the retail industry is in an unprecedented position of questioning whether traditional models can still provide competitive advantage. Furthermore, consumers are increasingly rocking back on their heels and questioning if the value exchange from providing personal data is indeed equitable and in their best interests.

To try and reset the balance and protect consumers' interests, the regulatory landscape has had to change with the times, including the introduction of data protection policies on a global scale to safeguard personal information. Meanwhile, the adoption of user-data-collecting devices (like IoT) aimed to enhance user

experience is increasing; yet these devices remain largely un-secure. For retailers, this means that protecting user data and creating a trusted relationship with customers while consistently encouraging them to share more information about themselves has never been more important.

To accomplish the above, as well as other potential requirements coming in the future, retail leaders should carefully compare digital identity management providers for customer identity and access management.

How to Use This Workbook

As part of the ForgeRock Ultimate Guide to Digital Identity Management for Customer Identity and Access Management Use Cases, this workbook follows two papers detailing the six digital transformation trends, components needed for customer identity and access management (CIAM) as well as future-forecasted use cases, and RFP questions and answers.

This workbook should be used in conjunction with the non-industry specific workbook *Comparing Digital Identity Providers for Customer Identity and Access Management*, which includes RFP questions based on basic and strategic CIAM components and capabilities.

Use this workbook to specifically compare digital identity management providers for the retail industry. The RFP questions in the section below are mapped to use cases, the context for each use case within the retail industry, and the associated CIAM components needed to address each use case and satisfy the RFP question. ForgeRock answers to the RFP questions are included within this workbook.

CIAM Questions to Ask Digital Identity Management Providers for the Retail Industry

Use Case and the Required CIAM Components	Retailer's Context	RFP Question
Use Case: Onboarding new customers **CIAM Components:** › Federated SSO › Social Registration › Self-Service › Login Analytics and Decision Logic › Progressive Profiling	Removing friction during user onboarding reduces barriers for consumers. Therefore, providing the most simple method of starting the onboarding process is key. Easy onboarding with a simple phone number and SMS verification allows customers to quickly onboard with an organization. Once onboarded, the ability to build a more complete picture of the user as they continue to interact through progressive profiling is critical. Progressive profiling then lets organizations gather additional user data throughout users' post-onboarding interactions.	Does the solution allow an easy onboarding experience using just a phone number and an SMS verification? Does the solution support additional onboarding scenarios for subsequent, progressive profiling steps along the customer journey?
Use Case: Modelling relationships **CIAM Components:** › Data Aggregation of People, Things, and Their Relationships	By modeling of families or smaller groups, organizations can better understand customers' relationships to other individuals for more targeted marketing, such as such as implementing loyalty cards to families for better marketing insights.	Can the solution map the relationships between individual customers, such as families or smaller groups?
Use Case: Delegating account access **CIAM Components:** › Authorization › Open Standards Support (UMA) › Privacy by Design and Consent mechanisms	In many scenarios, children who are below 18 years of age and live with their parents do not have a considerable amount of money, nor credit with a certain retailer, bank, or telecommunications company. Instead, they have loyalty cards that are attached to their parent's card. When the child's situation changes and they gain independence from their parents, the consumer relationship with the organization must be kept rather than being forgotten and losing the investment already built with the child consumer. When the relationship is lost, it results in a poor experience and lost opportunity.	Can the solution handle changes to families where, for example, a child moves from the parent household to his/her own household? This would require updating not only the family-child relationship (such as with a loyalty card) but also access permissions and so on.

Use Case and the Required CIAM Components	Retailer's Context	RFP Question
Use Case: Sharing identity information with third parties **CIAM Components:** › Federated SSO › Social Registration › Self-Service › Login Analytics and Decision Logic › Progressive Profiling	Consent-based sharing lets users share their information with third parties. The UMA 2.0 standard makes this capability possible. Being able to share information with third parties enables better personalization for marketing within the customer journey. It is also important in the era of GDPR and other data privacy regulations that prioritize choice and control for data subjects.	Can the solution allow consent-based sharing of an individual's shopping history with third parties using the UMA 2.0 standard?
Use Case: Standards based authentication **CIAM Components:** › Authorization › Multi-Factor Authentication › Next Generation AuthX (Authentication and Authorization)	Standards based authentication methods are mandatory for future proofing identity infrastructure. The United States National Institute of Standards and Technology (NIST) has established authentication assurance levels (AAL) to measure how strong a level of authentication is. For such assurance level determinations, it is important that digital identity providers support the NIST AAL authentication methods.	Does the solution support authentication methods layered by NIST AAL? Can the methods be used on mobile devices (iOS and Android)?
Use Case: Standards based authorization **CIAM Components:** › Authorization › Multi-Factor Authentication › Next Generation AuthX (Authentication and Authorization)	Standards based authorization methods are mandatory for future proofing identity infrastructure. The United States National Institute of Standards and Technology (NIST) has established a grading system called identity assurance levels (IAL). IAL measures the strength / trustworthiness of the evaluation criteria that ensures the user and their digital identity are one and the same. For such assurance level determinations, it is important that digital identity providers support the NIST IAL authorization methods.	Does the solution support authorization decisions based on NIST IAL? If the user does not have a certain IAL level, are they redirected to a verification service to obtain the required level?
Use Case: Connecting identity with API's **CIAM Components:** › Open Standards Support › Distributed Scope Design with Least Privileged Access › API First Model	The ability to interact with APIs, such as supporting a mobile loyalty app that has user-checkout functionality, is critical to enhancing the customer journey. Additionally, a solution should protect APIs. For example, in a PSD2 context, all access to financial APIs should be attached to an identity that is authenticated and authorized.	Does the solution interact with APIs and can it support apps such as a mobile loyalty app which has user-checkout functionality (such as allowing a user to scan a product's barcode within a physical store for self-serviced check-out)?
Use Case: Changing the customer journey based on risk profiles **CIAM Components:** › Multi-Factor Authentication › Zero Trust Security › Login Analytics and Decision Logic › Contextual Access	The ability to assess user access or to make purchases by utilizing adaptive risk characteristics and then applying step-up or multifactor authentication is a key enabler in adopting frictionless customer interactions. For instance, if a user is logging in via the same device previously used in the same geolocation with the same credentials, then they should be taken through one authentication process. However, if any of the characteristics such as device or location are different, then the process should result in a different authentication process determined by decision trees.	Does the solution support risk based profile management and adaptive risk balancing to mitigate fraud and enhance the user journey at various stages, including step-up authentication?

Use Case and the Required CIAM Components	Retailer's Context	RFP Question
Use Case: Terms and Conditions management **CIAM Components:** › Self-Service › Support for a Single View of Identities › Privacy by Design and Consent mechanisms	Terms and Conditions (T&Cs) capabilities make users accept T&Cs before they can access a service or application. This capability is important for auditing purposes and GDPR compliance.	Does the solution support tracking Terms and Conditions (T&Cs) acceptance? Further, does the solution track which user accepted which version of the T&C text as it is updated over time?
Use Case: GDPR **CIAM Components:** › Self-Service › Support for a Single View of Identities › Federated SSO › Privacy by Design and Consent mechanisms › Progressive Profiling	Some organizational brands are perceived as group-brands, while others are perceived as having no relation to a group. Organizations must store and manage customer data according to legislation and GDPR compliance. Therefore, a centralized overarching identity store is needed. If, however, a particular organizational brand wants to store data differently in one region versus another, or only wants to represent customer information from their particular brand, they should be able to do so. At the same time, organizations should also be able to provide the GDPR-mandated 'right to be forgotten' capability across multi-brand groups (associated brand entities) that the customer may engage in.	Does the solution support scenarios where each brand within a multi-brand group can decide how their data and visibility is managed?
Use Case: Personalization across multiple brands **CIAM Components:** › Self-Service › Support for a Single View of Identities › Federated SSO › Privacy by Design and Consent mechanisms › Progressive Profiling	Within the same overarching organization, retailers can benefit from account aggregation, allowing them to do things like collect shopping patterns across multiple brands in order to make their offering more personalized. For example, Business 1 is selling elegant clothing and Business 2 cosmetics. When a customer shops at Business 1 for an outfit, they could be offered matching cosmetics from Business 2.	Does the solution support account aggregation of a single consumer in multiple-brands? For example, if the consumer is enrolled with two different brands (Business 1 and Business 2) that are owned by the same overarching organization, can the solution determine on a group level that a user who identifies by their email address in Business 1 and by their loyalty card number in Business 2 is actually the same person?
Use Case: Developer friendly **CIAM Components:** › Zero Trust Security › System Integrations › API First Model	B2Developer channels enable developers to quickly deploy applications with identity built-in. Developers need quick and easy API access (this requires the generation of OAuth2 clientID/ClientCredentials). Therefore, the solution needs to be integrated in an external developer portal which is developed by the group.	Does the solution support B2Developer channels? Can the solution be integrated in an external developer portal which is developed by the group?
Use Case: Identity in loyalty programs **CIAM Components:** › Identity Store › Availability and Scale	Supporting multiple programs per customer, as well as instantaneous updating upon check-out, enables accurate aggregation and communication of data across all physical and digital touch-points.	Does the solution support multiple loyalty programs per consumer? Can the solution update all program data during the checkout process (physical and digital) so that potential benefits are visible immediately?

Use Case and the Required CIAM Components	Retailer's Context	RFP Question
Use Case: DevOps, Microservices, and API's **CIAM Components:** › API First Model › DevOps Friendly Architecture and Microservices › Legacy App Support	Retail companies have to consider moving from old legacy technology platforms as they continue to limit innovation. One compelling trend is for companies to adopt DevOps and build microservices. Moving from legacy platforms to microservices can be done as a transition. Therefore, the ability to extract identity from old monolithic applications and use this in new microservices is critical in the transition phase.	Does the solution provide the ability to abstract services from monolithic architectures to create new microservices, applications, or third party products and services that perform specialist tasks (for example: payment providers, logistics, rules engines, risks and fraud engines)?
Use Case: Identity consolidation and rationalization **CIAM Components:** › Support for a Single View of Identities › Data Aggregation of People, Things, and Their Relationships	By aggregating and providing a robust view of customer activities from multiple channels and engagements, an organization can gain a single view of a customer's identity across all channels.	Is the solution able to aggregate and provide a robust view of customer activities from multiple channels and engagements?
Use Case: Marketing personalization **CIAM Components:** › Strong Partner Ecosystem › System Integrations	For retailers who use third-party technology, ad serving, and marketing services, verifying the identity of the end recipient moves their business from general segment based to one-to-one marketing and ad serving. This adds significant value for both measuring the effectiveness of a campaign and delivering highly personalized content.	Does the solution enable and support the validation of identity through third-party ecosystems including marketing systems and other connected technologies?
Use Case: Physical to digital shopping channels **CIAM Components:** › Support for a Single View of Identities › Open Standards Support › Next Generation AuthX (Authentication and Authorization)	Retailers often lose their grip on the customer when traversing from physical to digital experiences. Solutions need to correlate the digital consumer with the person who is physically in a store and doesn't create a duplicate account where, for example, loyalty points are given to two different identities when it should be given to one. Likewise, the digital identity should be related with the physical one. Physical store technologies help to consolidate the physical and digital identity with in-store beacons localizers, smart applications, and others. Additionally, when users are shopping digitally, digital channel assistants like Alexa or Google Assistant not only allow for convenience, but can be applied to a wider audience, such as seniors, disabled people, and so on. Therefore, the ability to utilize these technologies is important.	Does the solution allow for an omni-channel solution to integrate physical and digital channels (also with respect to emerging technologies in the digital channel like voice assistance)?
Use Case: Data analytics **CIAM Components:** › System Auditing and Analytics	Retailers rely on big data analytics (BDA) tools for customer insight. Therefore, CIAM solutions should be able to integrate with analytics tools in order to analyze and leverage a user's full digital profile.	How does the solution interact with big data or other analytics tools?
Use Case: Cloud provision **CIAM Components:** › Multi-Cloud and Hybrid-Cloud Support › DevOps Friendly Architecture and Microservices	Retailers have many options when it comes to their cloud services and any CIAM solution should work effectively and portably with any cloud provider.	What cloud providers are supported by the solution?

This next section provides the RFP questions within the above tables along with the ForgeRock answer. Use the blank space to fill in other provider answers in order to make a direct comparison.

RFP Question	ForgeRock Answer	Other Provider Answer
Does the solution allow an easy onboarding experience using just a phone number and an SMS verification? Does the solution support additional onboarding scenarios for subsequent, progressive profiling steps along the customer journey?	Yes. ForgeRock fully supports a positive customer experience and easy onboarding with a simple phone number and SMS verification, as well as the use of progressive profiling to continuously gather additional data. By using Forgerock Access Manager and ForgeRock Identity Manager modules with custom stages to customize the registration experience, an organization can rapidly onboard new customers and continue to build a meaningful profile of them.	
Can the solution map the relationships between individual customers, such as families or smaller groups?	Yes. The ForgeRock Identity Platform enables companies to understand the complex nature of relationships between consumers, their family members, and small groups. Importantly, with the ForgeRock platform organizations can create a graph of these relationships. Once the relationships are understood, the ForgeRock Identity Platform can provide the authorization of sharing preferences and services across relationships and the ability to enable and disable sharing preferences and restrictions. For example, allowing a child to make purchases on a parent's account. Furthermore, if connected to a marketing automation system, known identity relationships can be utilized to improve marketing efficiency and target groups and families beyond traditional segmentation to provide truly personalized marketing.	
Can the solution handle changes to families where, for example, a child moves from the parent household to his/her own household? This would require updating not only the family-child relationship (such as with a loyalty card) but also access permissions and so on.	Yes. As well as managing user identities, the ForgeRock Identity Platform can manage relationships between identities. This can be used, for example, to manage relationships between a parent and a child, a teacher and their pupils, or an employee and their manager. Identities can also be created to represent any other thing or entity such as between a user and their devices, cars, organizations, companies, and services. The ForgeRock platform includes a tool to provide a visual display of the relationships between these identities.	
Can the solution allow consent-based sharing of an individual's shopping history with third parties using the UMA 2.0 standard?	Yes. ForgeRock was the first digital identity management provider to utilize the UMA standard. ForgeRock User-Managed Access is a standards-based privacy and consent solution based on the UMA 2.0 standard that gives end users a convenient way to determine who and what gets access to personal data, for how long, and under what circumstances.	
Does the solution support authentication methods layered by NIST AAL? Can the methods be used on mobile devices (iOS and Android)?	Yes, fully compliant. ForgeRock supports a wide range of authentication modules that can be configured together using authentication chains, and authentication nodes that can be configured together using authentication trees. ForgeRock push notifications can be used as part of the authentication process in ForgeRock Access Management, allowing multi-factor authentication or passwordless login via a mobile phone. The ForgeRock solution can model AAL (and IAL) as part of the authentication process. ForgeRock also supports post-authentication plugins to customize any process after the user or the entity has been authenticated.	

RFP Question	ForgeRock Answer	Other Provider Answer
Does the solution support authorization decisions based on NIST IAL? If the user does not have a certain IAL level, are they redirected to a verification service to obtain the required level?	Yes, fully compliant. With ForgeRock Intelligent Access, authentication trees can include nodes to increase the Identity Assurance Level (IAL) as opposed to the level of authentication. For example, users who authenticated using multi-factor authentication might still lack a level of identification. ForgeRock is able to detect this and to redirect the user to an appropriate identification service like VideoIdent.	
Does the solution interact with APIs and can it support apps such as a mobile loyalty app which has user-checkout functionality (such as allowing a user to scan a product's barcode within a physical store for self-serviced check-out)?	Yes, ForgeRock's solution supports mobile loyalty apps which have user-checkout functionality, such as allowing a user to scan a product's barcode within a physical story for self-serviced checkout.	
Does the solution support risk-based profile management and adaptive risk balancing to mitigate fraud and enhance the user journey at various stages, including step-up authentication?	Yes. The ForgeRock Identity Platform includes several approaches for performing risk-based authentication. With its Intelligent Access feature, workflow-like decision trees can be configured for an authentication journey. The nodes within the tree can take account of context factors such as location, IP address, device type, network or any other contextual information that is included in the request. The authentication trees provide fine-grained authentication by allowing multiple paths and decision points throughout the authentication flow. Additionally, with ForgeRock's Intelligent Access, authentication nodes can be added to an authentication tree in any position to either set or modify the authentication level. Controlling access to specific resources is done through authorization rules. ForgeRock Access Management has a policy engine which allows rules to evaluate the current authentication level and trigger step-up authentication if the user needs to access a more sensitive resource.	
Does the solution support tracking Terms and Conditions (T&Cs) acceptance? Further, does the solution track which user accepted which version of the T&C text as it is updated over time?	Yes. The ForgeRock Identity Platform provides a Terms and Conditions (T&Cs) capability out-of-the-box that can be configured so that users must accept the T&Cs before they can access a service or application. Admins can track and manage multiple versions of T&Cs and automatically prompt end users for their consent when T&Cs are updated to a new version. Different versions of T&Cs can be configured in multiple languages, with only the active version made visible to end users. Timestamp and versioning of T&Cs consented to is captured in the user metadata. Accepted T&Cs, along with the version number, can be found in the audit activity log. Alternatively, with ForgeRock's Intelligent Access, authentication trees can be configured to force new acceptance of T&Cs in order to complete the authentication journey.	

RFP Question	ForgeRock Answer	Other Provider Answer
Does the solution support scenarios where each brand within a multi-brand group can decide how their data and visibility is managed?	Yes. ForgeRock supports the management of domains or groups of users which can have their own branding. ForgeRock Access Management uses realms in order to implement the partitioning commonly required by multi-tenancy. Realms support delegated administration, with distinct groups of administrators only able to manage the realms they are configured to access. ForgeRock Identity Management is very lightweight and can be installed for each tenant separately. Therefore tenant data can be separated down to the log level. Integration with ForgeRock Access Management ensures that an administrator can log into multiple instances without re-authentication (SSO). ForgeRock Directory Services follows the standard LDAP model where different branches can be administered by different delegated admins. Here LDAP mechanisms such as access control items (ACIs) ensure that branches are protected against unauthorized access.	
Does the solution support account aggregation of a single consumer in multiple-brands? For example, if the consumer is enrolled with two different brands (Business 1 and Business 2) that are owned by the same overarching organization, can the solution determine on a group level that a user who identifies by their email address in Business 1 and by their loyalty card number in Business 2 is actually the same person?	Yes. ForgeRock's Identity Platform can differentiate between accounts and identities. Therefore, a single user/identity can have multiple accounts within a group-brand. ForgeRock also allows users to authenticate using the credentials from one brand's account to all other brands' accounts within the group-brand. Further, ForgeRock provides tools to automatically correlate an account to an already existing identity.	
Does the solution support B2Developer channels? Can the solution be integrated in an external developer portal which is developed by the group?	Yes. ForgeRock provides a fully-fledged API solution to allow third parties to securely leverage the identity system. This gives access to certain data in order to build new business ideas and services. ForgeRock fully supports B2Developer channels by REST-ful APIs as a first-class citizen.	
Does the solution support multiple loyalty programs per consumer? Can the solution update all program data during the checkout process (physical and digital) so that potential benefits are visible immediately?	Yes. ForgeRock can keep track of all the loyalty programs as user has. For example, ForgeRock's high performance directory server can provide a datastore for storing the information and make it quickly available to leverage a fast and user friendly checkout, even for physical storefronts.	
Does the solution provide the ability to abstract services from monolithic architectures to create new microservices, applications, or third party products and services that perform specialist tasks (for example: payment providers, logistics, rules engines, risks and fraud engines)?	Yes. The ForgeRock Identity Platform integrates with different uses of a microservices architecture, including consumer-to-service and service-to-service. Microservices might be REST endpoints, although they do not have to be. Services can be fronted by ForgeRock Identity Gateway in order to externalize the token validation and access control, much like a traditional web application can. This ensures any request the traditional web app receives is using a validated authentication context, including an identity of a subject known to the environment. ForgeRock Identity Gateway may have access to the ForgeRock Access Management session information, which it can validate in order to determine the identity and authorization of the calling user.	

RFP Question	ForgeRock Answer	Other Provider Answer
Is the solution able to aggregate and provide a robust view of customer activities from multiple channels and engagements?	Yes. With the ForgeRock Identity Platform, organizations can build a solution that enables activities across different channels and engagements. For example, unique transaction IDs can be used to track which internal services a user accessed using which device. This can help organizations to understand potential weaknesses in their own platform. For example, if the same user always fills their shopping basket via a desktop browser, but checks out via a mobile phone, this could suggest that the organization's catalog pages are not optimized for mobile devices.	
Does the solution enable and support the validation of Identity through third-party ecosystems including marketing systems and other connected technologies?	Yes. ForgeRock links identities from different systems to create a single version of a user's identity. If users have more then one social identity provider, they can link them to the same user account from the self-service UI. In cases where there are existing repositories of user data, ForgeRock Identity Management can use these to create a single unified profile of each user through the use of the synchronization engine. Typically this is done in an automated way using data matching association rules. For example, a marketing tool is able to leverage data about the user that lives outside the marketing system (assuming the user consented to the usage). This allows for a more personalized marketing strategy by taking advantage of the available identity attributed.	
Does the solution allow for an omni-channel solution to integrate physical and digital channels (also with respect to emerging technologies in the digital channel like voice assistance)?	Yes. ForgeRock supports the OAuth2 device flow and many other emerging standards within the OAuth2 ecosystem that are not part of the normal OAuth2 core specification. This allows the integration of devices and modeling of use cases that would otherwise be impossible without leaving the standard.	
What cloud providers are supported by the solution?	The ForgeRock Platform can be deployed on any cloud environment (including multi-cloud, hybrid-cloud, and bring-your-own-cloud) in minutes with preconfigured cloud installation packages of 1M, 10M, and 100M identities. Cloud environments include, but aren't limited to, Amazon Web Services, Google Cloud, OpenShift, and Microsoft Azure. ForgeRock also offers its identity platform as a service. This provides the full power and of the ForgeRock Identity Platform while minimizing the overheads of installation, operation and maintenance. It is important to note that the ForgeRock's PaaS service is not a cut-down or limited features version of our platform and offers flexibility that more constrained SaaS vendors would struggle to provide. Additionally and importantly, the ForgeRock PaaS and software offerings share the same code base.	

For additional RFP questions to ask digital identity management providers for CIAM, as well as an in-depth review of the components providers should offer, read *Comparing Digital Identity Management Providers for Customer Identity and Access Management*.

ForgeRock: Defining Digital Identity Management

Identified as an customer identity and access management (CIAM) platform Overall Leader by KuppingerCole and one of the most visionary access management provider by Gartner, the ForgeRock Identity Platform is shaping the future of digital identity management.

The ForgeRock Identity Platform is a simple yet comprehensive digital identity management solution that can be implemented across an organization for all use cases — employees, customers, devices, and 'things'. The ForgeRock Identity Platform consists of access management, user-managed access, identity management, governance, automated identity, directory services, edge security, and an identity gateway. The full platform can be consumed as a service (PaaS) or deployed in minutes within any cloud environment, including multi-cloud and hybrid-cloud, for millions of identities. Importantly, the ForgeRock Identity Platform is the only solution on the market able to address all components of the six global trends and beyond. Read why in *Evaluating Digital Identity Providers for Customer Identity and Access Management: Top Criteria, Differentiators, and Questions to Ask CIAM Providers.*

Learn More About ForgeRock for Your Organization

ForgeRock is an overall leader and most visionary digital identity management provider. Contact us to learn how ForgeRock can help your organization.