ForgeRock

CIAM

How to Compare Digital Identity Management Providers for CIAM Within the Auto and New Mobility Industry

A Workbook

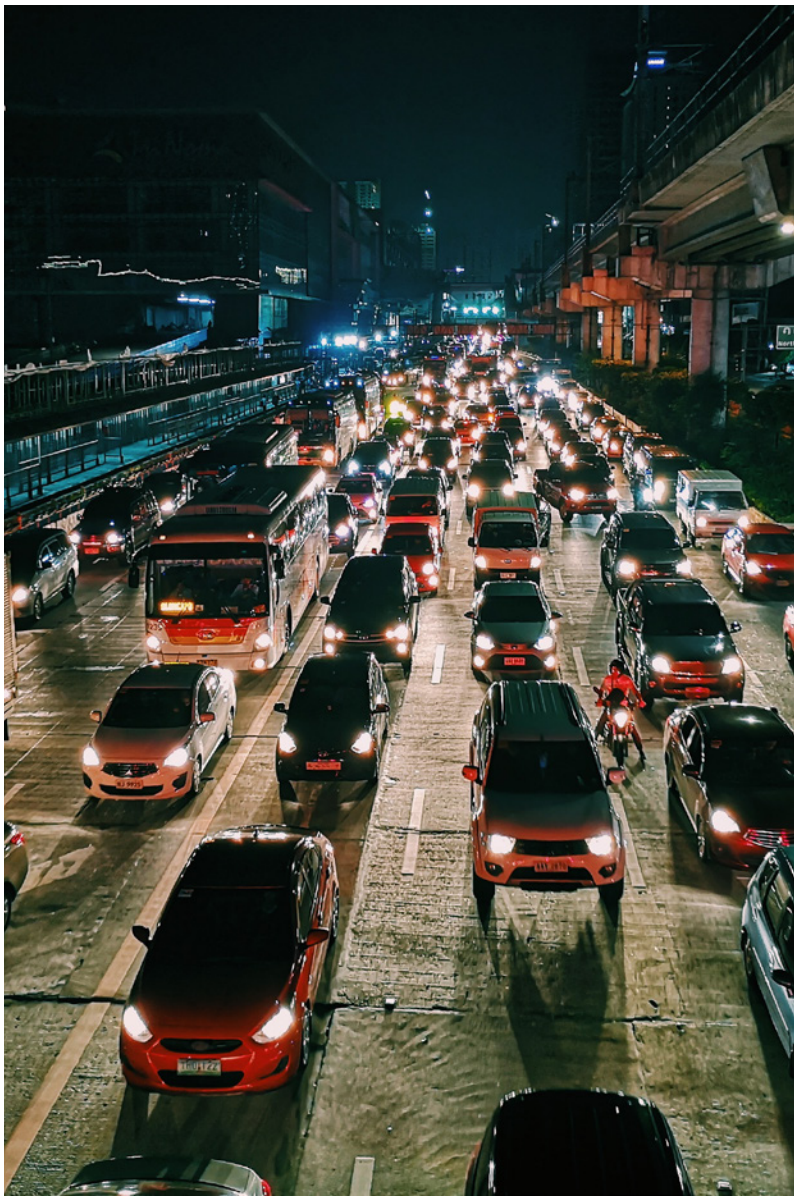
The auto and new mobility industry is changing faster than ever before. Today, the industry has billions of clients and interacts directly with both the physical and digital ecosystems. Additionally, the industry is influenced by six digital transformation trends:

- **The Disruptive Economy:** The combination of ingenuity and technology has created a high-stakes game to capture consumer attention. This means constantly reinventing offerings to surprise and delight customers. Mobility companies such as Lyft and Uber have changed the way clients perceive mobility. And, in the not-so-distant future, the autonomous car will hit the market. There is also a race for superiority within electric and energy efficient capabilities.
- **Internet of Things (IoT):** Vehicles are now IoT 'things' that connect to thousands of other IoT and smart components, such as virtual keys, satellites, and mobile phones, as well as to integrated environments/

architectures such as 'smart cities'. Secure connectivity and associations between the vehicle, the manufacturer's infrastructure, the cloud, the driver, and pedestrians is a necessity.

- **Cybercrime and over-reach:** The number of data breaches, hacks, ransomware, and discoveries of over-reach have skyrocketed with no sign of relenting. Within the automotive ecosystem, connected electronic components and IoT connected services must be safe and secure.
- **Public opinion:** Public opinion has taken a defensive turn. Consumers want control of their personal data and for organizations to be held accountable when there is a breach of trust. Additionally, consumers are increasingly demanding energy efficient and electric vehicles and desire to orient themselves with manufacturers that are environmentally and sustainably minded, as well as with those with reputations they can trust with their personal data.

To address the digital transformation trends within the auto and new mobility industry, leaders need to ensure they are able to address the needs of today as well as tomorrow.



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 and the components needed for customer identity and access management (CIAM), as well as future-forecasted use cases.

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 auto and new mobility industry by copying the RFP question tables and filling in the blank answer boxes provided. ForgeRock answers are included within this workbook.

CIAM Questions to Ask Digital Identity Management Providers for the Auto and New Mobility Industry

Provider:

Question	Reason This Is Important To Ask	Answer
What is the role and value of digital identities in new and upcoming automotive business models?	It is important to understand the level of expertise the digital identity provider has within the automotive and new mobility industry. Within digital identity, it's not just the product features that makes a provider a "good provider". The provider should be highly involved within the automotive and new mobility industry enough to fully understand the scale, challenges, and specific requirements of the market today as well as tomorrow. This includes industry trends (connectivity, privacy, IoT), commercial users for fleet management, and consumers.	
What are the key digital identity features for the automotive and new mobility industry?	It is important to know what digital identity providers believe are the most important features for the automotive industry in order to assess which provider shares a common vision.	
How does your solution support today and tomorrow's data privacy regulations, such as consent management? Does the solution leverage the UMA 2.0 standard?	Automobiles are now inter-connected devices, both collecting and using personal data. Because of this and regulations such as GDPR, it is imperative that a digital identity provider offer dynamic privacy and consent features as part of their solution. It is also important that digital identity providers have a plan to address future forecasted regulations. The UMA standard is a lightweight access control protocol that defines a centralized workflow to allow an entity (user or corporation) to manage access to their resources. UMA extends the OAuth 2.0 protocol and gives resource owners granular management of their protected resources by creating authorization policies on a centralized authorization server, such as ForgeRock Access Management. The authorization server grants delegated consent to a requesting party on behalf of the resource owner to authorize who and what can get access to their data and for how long.	
How does your solution provide users with the capability to manage privacy and data sharing?	Data sharing between a car manufacturer, customer, and other third parties such as insurance companies needs to be secure and comply with regulations. This means that users must provide consent for data sharing. For example: if a car manufacturer wants to sell customer data to an insurance company, they must ensure consent is given by the customer to share the data with the insurance company. Further, the car manufacturer must also provide the capability for the user to only share their data for a specific use case. This may require the User Managed Access (UMA) 2.0 standard in combination with an identity relationship engine.	

Question	Reason This Is Important To Ask	Answer
How does the solution scale to meet peaks in demand for authentication and authorization?	The number of people, cars, devices, IoT intelligent 'things' are now in the billions with a high level of segregation. Additionally, automobiles are used cross-regionally. Hence, not only is it important for a digital identity provider to support authentication and authorization at a massive scale, but to also do so with ease during peaks in demand, such as rush hours.	
How does the solution connect cars and customers with the overall ecosystem of applications, devices, and services? **Does the solution provide API and standard based flows to enable an ecosystem for connections between auto-makers and suppliers?**	One of the main challenges between auto-makers and suppliers is the integration between their respective services, resulting in one integration every time the two connect. Therefore, the way forward is to define and build a mobility and automotive-specific integration/API marketplace in order to enable an ecosystem of connection and relationship.	
Does the system support biometric authentication or biometric-involved authentication, such as fingerprint readers, TouchID, facial recognition, etc.? Please elaborate.	Members and patients should be able to use passwordless login methods to quickly engage with services or applications.	
Does the solution support biometric authentication or biometric-involved authentication, such as fingerprint readers, TouchID, and so on? Please elaborate.	User authentication for both automobiles and the devices that are integrated with them is crucial. Additionally, the ability to have a secure and seamless experience is mandatory. To enable this, biometric authentication (such as fingerprint readers, TouchID, etc.) capabilities and versatility provide the core components for a virtual key system, as well as authorization capabilities. Therefore, a digital identity management solution needs to be able to connect to biometric authentication schemes — whether through proprietary handset makers or auto makers.	
Does the solution include identity relationship modeling?	Identity relationship modeling is the ability to model and manage relationships between identities, such as between parents and their children. Within the auto and new mobility industry, it is important to understand the relationships between cars, drivers, owners, passengers, devices, and smart city infrastructures as they are dynamic links that live within the industry ecosystem. As part of a digital identity solution, identity relationship features not only enhance user experience and brand loyalty through content personalization and recommendation, but also enable different monetization models relating to groups of related people and things. This allows for end-to-end intermodal mobility.	
How does the solution integrate with an IoT platform?	The architecture and ecosystem of the 'connected car' is made up of the connected relationships between cars, car parts, owners, drivers, passengers, devices, and smart city infrastructure. Therefore, digital identity management support for devices, IoT 'things', and services through an automotive-specific IoT platform is vital for managing the digital relationships and technical components between all of the above. This support enables a personalized experience and also secures access for automated consumption of microservices in machine-to-machine environments.	

Question	Reason This Is Important To Ask	Answer
Does the solution provide risk and/ or value based authentication (adaptive authentication), enabling apps to have different levels of credentials to authenticate against a common identity store?	Risk management for automotive and new mobility use cases is key. It is particularly important within the car sharing business model. Whether it's an end-user's credit worthiness, a renter's lease history, or some other risk measurement, — checking the risk before authorizing services is essential. A digital identity solution should combine risk-based / adaptive authentication and authorization to enable decisions regarding permission and entitlement to be made in context throughout the customer journey. For example, based on a contextual risk assessment, a simple username and password will suffice for some users, while for others a 6-digit code sent to a mobile device and entered into the app is required. This not only improves security, but also provides a better user experience for the customer.	
Is the solution capable of integrating with payment services?	To support the ability for users to pay for services such as gas, tolls, in-dash purchases, and even drive-through restaurant orders directly through their automobile, a digital identity solution needs to include a payment service. To do this, the automobile-specific identity solution should be easily linked (or federated) with the end user's payment identity.	
Is the solution capable of integrating with automotive services such as online maps, navigation updates, music streaming, and auto software updates?	To be relevant within today's auto and new mobility market, auto makers must enable end-user connectivity for 'infotainment' services, as well as auto-specific software updates, etc. This necessity results in a customer-specific requirement for data bandwidth and volume. An auto and new mobility-minded digital identity solution should support the ability to 'broker' a user's personal service subscription, such as a music streaming service, so that the user can access it using the automobile itself. The subscription is a digital identity, and as such is provided by a mobile network operator (MNO). The digital identity solution then links the subscription identity to the digital identity of the vehicle.	

Provider: ForgeRock

Question	Reason This Is Important To Ask	ForgeRock Answer
What is the role and value of digital identities in new and upcoming automotive business models?	It is important to understand the level of expertise the digital identity provider has within the automotive and new mobility industry. Within digital identity, it's not just the product features that makes a provider a "good provider". The provider should be highly involved within the automotive and new mobility industry enough to fully understand the scale, challenges, and specific requirements of the market today as well as tomorrow. This includes industry trends (connectivity, privacy, IoT), commercial users for fleet management, and consumers.	The automotive and new mobility industry is a focus for ForgeRock. Forgerock has been engaged in Automotive/new mobility since 2016. Initially starting with an engagement in AGL (Automotive Grade Linux) followed by an active membership in CCC (Car Connectivity Consortium). AGL is already solving the software development issues associated with high-tech infotainment systems in modern vehicles, and we believe this same group of passionate members can create solutions to other pressing issues that OEMs are facing, such as monetizing services through their vehicle platform to create a key revenue stream in addition to selling vehicle units. Using the Forgerock Identity Platform, auto and new mobility customers manage millions of identities within the industry. Additionally, ForgeRock is well on the way to bring digital identity to the connected vehicle ecosystem, to help OEMs build strong relationships with their customers and to empower OEMs to meet modern consumers expectation on privacy and consent as well as allowing granular access to data.

Question	Reason This Is Important To Ask	ForgeRock Answer
What are the key digital identity features for the automotive and new mobility industry?	It is important to know what digital identity providers believe are the most important features for the automotive industry in order to assess which provider shares a common vision.	ForgeRock has identified the main digital identity features to support automotive and new mobility trends as being (1) Privacy: to ultimately move from anonymous data to PII and enable data sharing with consent, monetization, (2) Relationships: to efficiently utilize the relationships of people, cars, devices, things, and objects in the magnitude of 100s of millions, and (3) an Open Marketplace: that allows automotive organizations to share and monetize data across car brands and across industries (auto, telco, retail, financial services, and so on) in order to deliver a consumer-centric experience.
How does your solution support today and tomorrow's data privacy regulations, such as consent management? Does the solution leverage the UMA 2.0 standard?	Automobiles are now inter-connected devices, both collecting and using personal data. Because of this and regulations such as GDPR, it is imperative that a digital identity provider offer dynamic privacy and consent features as part of their solution. It is also important that digital identity providers have a plan to address future forecasted regulations. The UMA standard is a lightweight access control protocol that defines a centralized workflow to allow an entity (user or corporation) to manage access to their resources. UMA extends the OAuth 2.0 protocol and gives resource owners granular management of their protected resources by creating authorization policies on a centralized authorization server, such as ForgeRock Access Management. The authorization server grants delegated consent to a requesting party on behalf of the resource owner to authorize who and what can get access to their data and for how long.	The ForgeRock Identity Platform provides a comprehensive set of end-user privacy capabilities that can help address many GDPR topics such as obtaining and storing consent, purpose limitation, data minimization, and data accuracy. ForgeRock User-Managed Access (UMA) is a privacy and consent solution based on the UMA 2.0 standard that helps address compliance with consent requirements of privacy laws. With its out-of-the-box UMA capabilities, the ForgeRock Platform allows users to manage — grant and withdraw — consents and permissions in a fine-grained fashion over time from a convenient, central console across multiple data services. UMA capabilities are available in ForgeRock Access Management (authorization server), ForgeRock Identity Gateway (resource server), and through the Profile and Privacy Management dashboard in ForgeRock Identity Management. This user-centric approach addresses GDPR concepts of consent and data minimization. UMA capabilities also enable users control of access to APIs. The approach of protecting APIs that directly deliver data to processors without central aggregation addresses the GDPR concept of data accuracy. The ForgeRock Platform can also capture user consent with Terms and Conditions (T&Cs) and privacy notices during both account registration and authentication. The platform also enables users to manage account information over time.
How does your solution provide users with the capability to manage privacy and data sharing?	Data sharing between a car manufacturer, customer, and other third parties such as insurance companies needs to be secure and comply with regulations. This means that users must provide consent for data sharing. For example: if a car manufacturer wants to sell customer data to an insurance company, they must ensure consent is given by the customer to share the data with the insurance company. Further, the car manufacturer must also provide the capability for the user to only share their data for a specific use case. This may require the User Managed Access (UMA) 2.0 standard in combination with a relationship engine.	ForgeRock User-Managed Access provides a convenient central console for organizing digital resources residing in many locations, delegating scoped access to others, and monitoring and revoking access. From a dedicated landing page the end user can grant requests, edit the scopes granted, and deny requests. Chained delegation enables a resource requester to re-share it with another requester, with the entire access history visible to the original owner who can deny requests by revoking the original policy. Administrators can set realm-level features such as access token expiration times and email notifications surrounding pending access requests. Implementers can use extensive API endpoints and plug-in points to customize just about any characteristic of the UMA provider, including the user interface.

Question	Reason This Is Important To Ask	ForgeRock Answer
How does the solution scale to meet peaks in demand for authentication and authorization?	The number of people, cars, devices, IoT intelligent 'things' are now in the billions with a high level of segregation. Additionally, automobiles are used cross-regionally. Hence, not only is it important for a digital identity provider to support authentication and authorization at a massive scale, but to also do so with ease during peaks in demand, such as rush hours.	The ForgeRock Identity Platform was designed from the ground up to provide telco-grade scalability and availability. The ForgeRock Identity Platform supports both CTS-based (stateful) and client-based (stateless) sessions. Being Java-based, threaded, and transactional in nature, the ForgeRock suite of products handles both vertical and horizontal scaling particularly effectively. Vertical scaling involves the use of multiple processors/cores on a given operating system installation. The Java environment can automatically leverage all processors/cores within a system. Horizontal scaling leverages multiple independent operating system instances which have commonly configured ForgeRock products. An external load balancer is used to distribute the workload across all configured systems. Additional CPU and memory in a given server will typically increase throughput linearly (assuming no other external factors), while additional servers in a load-balanced farm will similarly increase throughput in a predictable, linear fashion.
How does the solution connect cars and customers with the overall ecosystem of applications, devices, and services? **Does the solution API and standard based flows to enable an ecosystem for connections between auto-makers and suppliers?**	One of the main challenges between auto-makers and suppliers is the integration between their respective services, resulting in one integration every time the two connect. Therefore, the way forward is to define and build a mobility and automotive-specific integration/API marketplace in order to enable an ecosystem of connection and relationship.	ForgeRock Identity Management provides a rich environment for managing users and arbitrary custom objects (called managed objects), and the relationships between them. This is used, for example, to create a managed object type representing devices, with all the necessary device attributes, and the relationships between users and their devices. A full REST interface (and web UI) is provided to manage the lifecycle of managed objects, and if appropriate, workflows or synchronization with other data stores. Almost all commercial API gateways have adopted identity standards such as OAuth and OpenID Connect in order to authenticate and authorize access to APIs and resources. The ForgeRock Identity Platform fully supports these standards.
Does the solution support biometric authentication or biometric-involved authentication, such as fingerprint readers, TouchID, and so on? Please elaborate.	User authentication for both automobiles and the devices that are integrated with them is crucial. Additionally, the ability to have a secure and seamless experience is mandatory. To enable this, biometric authentication (such as fingerprint readers, TouchID, etc.) capabilities and versatility provide the core components for a virtual key system, as well as authorization capabilities. Therefore, a digital identity management solution needs to be able to connect to biometric authentication schemes — whether through proprietary handset makers or auto makers.	Biometric authentication is a fast evolving sector in the industry. ForgeRock supports iOS and Android fingerprint and facial recognition as part of its push notification authentication service, where local device sensors are required to acknowledge the user's response to the notification. Furthermore, ForgeRock maintains technology partnerships with a growing number of vendors specializing in biometric technologies. Through the ForgeRock Trust Network, a technology partner program, we provide a marketplace where customers can discover third-party identity and access management technologies that are commonly used in conjunction with each other. A full list of our technology partners can be found on the ForgeRock website. The ForgeRock architecture allows for integration of biometrics-based authenticators through open standards and APIs, leveraging standard protocols such as OpenID Connect and SAML, or leveraging API-based integration via a scriptable authentication node. By providing an extensibility framework, the ForgeRock platform can integrate with various biometric authenticators, including FIDO compliant authenticators. Integration of third party authentication technologies, such as biometric readers, can be achieved through documented integration points. For light-touch integration, a scripted authentication node might be suitable, whereas for close integration, a full authentication node may be more appropriate.

Question	Reason This Is Important To Ask	ForgeRock Answer
Does the solution include identity relationship modeling?	Identity relationship modeling is the ability to model and manage relationships between identities, such as between parents and their children. Within the auto and new mobility industry, it is important to understand the relationships between cars, drivers, owners, passengers, devices, and smart city infrastructures as they are dynamic links that live within the industry ecosystem. As part of a digital identity solution, identity relationship features not only enhance user experience and brand loyalty through content personalization and recommendation, but also enable different monetization models relating to groups of related people and things. This allows for end-to-end intermodal mobility.	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. For convenience, the ForgeRock Identity Platform predefines certain types of identity objects including both user identities, and roles, so that it is quick and easy to relate users with roles, or any other combination. Adding additional object types, or modifying the predefined types is also trivial and common practice.
How does the solution integrate with an IoT platform?	The architecture and ecosystem of the 'connected car' is made up of the connected relationships between cars, car parts, owners, drivers, passengers, devices, and smart city infrastructures. Therefore, digital identity management support for devices, IoT 'things', and services through an automotive-specific IoT platform is vital for managing the digital relationships and technical components between all of the above. This support enables a personalized experience and also secures access for automated consumption of microservices in machine-to-machine environments.	ForgeRock supports open standards and APIs, and can integrate with AWS IoT and similar platforms. The ForgeRock Identity Platform addresses requirements for many aspects of IoT security. These include communication security, data at rest security, payload protection, data in transit encryption, authentication, authorization, and audit logging. ForgeRock developed a specific IoT module called the identity edge controller (IEC). With this module devices are treated as first class citizens, giving 'smart things/devices' all the capabilities a user would have.
Does the solution provide risk and/ or value based authentication (adaptive authentication), enabling apps to have different levels of credentials to authenticate against a common identity store?	Risk management for automotive and new mobility use cases is key. It is particularly important within the car sharing business model. Whether it's an end-user's credit worthiness, a renter's lease history, or some other risk measurement, — checking the risk before authorizing services is essential. A digital identity solution should combine risk-based / adaptive authentication and authorization to enable decisions regarding permission and entitlement to be made in context throughout the customer journey. For example, based on a contextual risk assessment, a simple username and password will suffice for some users, while for others a 6-digit code sent to a mobile device and entered into the app is required. This not only improves security, but also provides a better user experience for the customer.	Risk-based authentication (or adaptive authentication) is natively supported in ForgeRock's Intelligent Access, delivered through an authentication trees framework. With ForgeRock Intelligent Access, 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. Based on the outcome, nodes can be configured for risk calculations, modifications to authentication level, alteration of session properties, and more. Administrators can use digital signals to design a smart login journey that minimizes friction and maximizes security for legitimate users while suspicious users could be denied access or redirected to a sandbox environment for further monitoring.

Question	Reason This Is Important To Ask	ForgeRock Answer
Is the solution capable of integrating with payment services?	To support the ability for users to pay for services such as gas, tolls, in-dash purchases, and even drive-through restaurant orders directly through their automobile, a digital identity solution needs to include a payment service. To do this, the automobile-specific identity solution should be easily linked (or federated) with the end user's payment identity.	The ForgeRock Identity Platform can enable organizations to secure payment transactions through payment services APIs and can reduce the risk associated with them. The payment API must first be protected, either with ForgeRock Identity Gateway handlers, another standards compliant API gateway, or through writing code. ForgeRock Access Management can then be used as a PDP that enforces strong authentication, for example through step-up authentication or transactional authorization. ForgeRock provides a full support of the latest standards used in OpenBanking and PSD2. ForgeRock also offers an OpenBanking Sandbox to help providers test functionality within a safe environment. ForgeRock also provides an implementor kit that includes APIs and connectors to quickly implement such initiatives. Some of the largest banks within the industry rely on ForgeRock for OpenBanking and PSD2.
Is the solution capable of integrating with automotive services such as online maps, navigation updates, music streaming, and auto software updates?	To be relevant within today's auto and new mobility market, auto makers must enable end-user connectivity for 'infotainment' services, as well as auto-specific software updates, etc. This necessity results in a customer-specific requirement for data bandwidth and volume. An auto and new mobility-minded digital identity solution should support the ability to 'broker' a user's personal service subscription, such as a music streaming service, so that the user can access it using the automobile itself. The subscription is a digital identity, and as such is provided by a mobile network operator (MNO). The digital identity solution then links the subscription identity to the digital identity of the vehicle.	Yes. The ForgeRock platform has the capability to treat devices as first class citizens giving the car a single or multiple trusted and unique identities. These identities can be used to uniquely identify not just the car itself but individual car subsystems. Fine grained access to updates, upgrades, value add services and a payment process can be managed and secured.

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*.

Notes:

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 providers 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 that fully supports *all components needed to address the six global trends and beyond.*

Learn More About ForgeRock for Your Organization

ForgeRock is the leading and most visionary digital identity management provider. Contact us to learn how ForgeRock can help your organization.