ForgeRock

CIAM

Comparing Digital Identity Management Providers for Customer Identity & Access Management

A Workbook

How to Use This Workbook

Use this workbook to:

- Review the six digital transformation trends and the components needed for customer identity and access management (CIAM), as well as future-forecasted use cases.
- Ask digital identity management providers RFP questions and capture their answers and capabilities in the Comparing Digital Identity Management Providers sections.

Why Digital Identity Platforms for Customer Use Cases? A Contextual Review

Within the past decade, there has been an explosive combination of technology and ingenuity — culminating in six global trends that are actively and interdependently shaping business and society today. Anchored in customer experience and demand, these trends are now the landscape that organizations must navigate. To survive and thrive, organizations must be equipped to address each.

1. 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.

2. Internet of Things (IoT)
By 2020 there will be 25 billion connected 'things'. Unfortunately, most 'things' are not secure.

3. Cybercrime and over-reach
The number of data breaches, hacks, ransomware, and discoveries of over-reach have skyrocketed with no sign of relenting.

4. Public opinion
Public opinion has taken a defensive turn. Consumers want control of their personal data and for organizations to be held accountable.

5. Changing regulatory environment
The General Data Protection Regulation (GDPR) is the most profound regulation passed since the 1990s, changing business globally. Additional regulations (Open Banking, PSD2) have passed and more are expected to follow.

6. Gen Z and Gen Alpha
By 2020, Generation Z will become the largest consumer group in the US and Europe. Behind them, Gen Alpha already has household purchase influence. Unfortunately, the above presents real challenges to current organizational ecosystems.

For an in-depth review of the top six trends, read: *The Top Six Digital Transformation Trends Shaping Business and Society: Why Digital Identity Platforms Are the New Imperative for Customer Identity and Access Management*

Supporting the Six Trends' Customer Use Cases

In terms of the customer use cases defined by the six trends, the most advanced digital identity platforms must enable organizations to:

- Personalize customer experiences, build relationships and, deliver omnichannel experiences
- Secure and connect billions of customer and IoT identities and data
- Authenticate and authorize billions of logins and transactions daily
- Facilitate security, analytics, privacy, and control
- Support and adhere to regulations (GDPR, HIPAA, Open Banking, PSD2)
- Integrate with other systems, such as marketing automation systems
- Easily scale to meet demands and requirements
- Identify and protect against fraudulent or malicious activities

Seven Basic Components for Customer Identity and Access Management

Behind the scenes, digital identity management platforms are now the enablers of both business and everyday life. Yet, platforms vary in their components and capabilities. The following are the seven basic components of digital identity management platforms needed to begin to address the six global trends.

To help evaluate providers for each component, RFP questions are provided on pages 8-10. Fill in provider answers in the sections at the end of this workbook. Stay tuned for industry-specific workbooks that include questions by the healthcare, automotive and new mobility, retail, telecommunications, and financial services industries.

Basic Component	Description
Federated SSO	Based on trusted relationships between organizations, federated single sign-on (SSO) gives users secure access to those organizations' web properties and applications using a single account, hence single sign-on. Federated SSO uses open standards such as OAuth, WS-Federation, WS-Trust, OpenID Connect and SAML to pass authentication tokens between the organizations' identity providers.
Social Registration and Authentication	As a form of single sign-on (SSO), social registration and authentication allows users to register and authenticate quickly and easily using their existing information from a social networking service, such as Google or Facebook.

Basic Component	Description
Multi-Factor Authentication	Multi-factor authentication (MFA) is a method of validating a users identity through multiple authentication mechanisms. Authentication mechanisms include something the user knows, something the user has, and something the user is. For example, access is only granted after a user enters their password (what the user knows) and a numeric code sent by text to their phone (something the user has).
Authorization	As part of access control within a digital identity solution, authorization is the function of determining if a user has permission to access a specified resource(s), such as a website(s), record(s), document(s), and so on.
Self-Service	'Self-service' refers to allowing users to manage their accounts on their own rather than relying on an organization's support staff. Examples of self-service include managing login preferences, password management, updating contact information, requesting support, and so on. Self-service not only reduces support costs, it also improves user experience and customer engagement.
Identity Store	As part of Directory Services, an identity store is a repository for the attribution data of identities. Stored identity data should be encrypted both while at rest and in transit. Also, as a best practice, it is good to have an embeddable repository that can easily share real-time customer, device, and user identity data across multiple environments. Additionally, from a hosting perspective, identity stores should include high availability, performance, and security. Also, the identity store should be fully compliant with LDAP v3 and should integrate seamlessly with any directory.
Support for a Single View of Identities	A single view of a customer (an identity) organization-wide improves security, customer service, marketing initiatives, and more. For digital identity platforms to support 'a single view of identities', they must have the ability to integrate with other systems and consolidate multiple customer data silos in order to create a single view organization-wide.

Beyond the Basics: Strategic Components for Customer Identity and Access Management

To do their job well, digital identity platforms should go 'beyond the basics' and contain strategic technology components designed to not only address the current six global trends, but those to come. The following are the strategic components digital identity platforms must provide in order to meet today's six global trends and beyond.

Strategic Component	Description
Availability at Scale	It is important to ensure that a user's access and session remains undisrupted should something happen, such as a server going down. Digital identity providers should support both 'service availability' and 'session availability'. Service availability ensures users can access a site when a server goes down. Session availability preserves and keeps a session running if a server goes down. Digital identity providers should also support a variety of scale scenarios. This includes a shifting number (often millions) of users, devices, and things that need to be stored in a database, as well as changing frequencies and lengths of simultaneous and concurrent sessions. Support for a stateless protocol using JWT session tokens is also advisable.
Open Standards Support	Open standards are established, uniform technical norms used by developers. Each standard has specified capabilities and functionality. Identity security relies on the OAuth2, OpenID Connect, and SAML standards. Going beyond these basic identity standards, leading digital identity providers are integrating standards that are needed to support the six global trends, such as UMA 2.0, which allows users to securely share access to personal data with a third-party. Other advanced standards include OAuth 2.0 Proof-of-Possession, which ensures that the presenter of a bearer token is the real and original token owner, and OAuth2 Device Flow, which is designed for client devices that have limited user interfaces.

Strategic Component	Description
Zero Trust Security	The Zero Trust Security model is based on the idea that no network, individual, 'thing', or device can be trusted. Digital identity platforms should be able determine whether an entity requesting an action is authorized to do so, and if they have proven they are the entity they claim to be with a sufficient level of assurance based on the risk of the specific action. Within a Zero Trust Security model, every action taken must be properly authenticated and authorized. To do this, authentication and authorization decisions leverage contextual information and become risk-based rather than binary, taking into consideration a rich set of information.
Distributed Scope Design with Least Priviledged Access	Scopes enable the principle of 'least privileged access'. This means only granting access that is essential to perform an intended purpose. For example, customers are only permitted to access the exact information and resources necessary for a particular and legitimate purpose. A first step towards achieving this fine-grained authorization is developing a mechanism to 'distribute' and assign strongly-typed scopes to applications, API endpoints, and other protected resources. Scopes must then be coupled with real-time context at policy-enforcing gates throughout the identity ecosystem. Scopes for fine-grained, actionable rules that can be used to make authorization decisions should also be applied.
Contextual Access	Most identity solutions only protect at the initial authentication. To ensure the authenticity of users, devices, 'things', and services at all times and mitigate risk whenever an anomaly is detected, even during existing sessions, contextual access should be applied. As part of Next Gen AuthX, contextual access builds context-based intelligence into policies to assess risk and protect resources at the time of access as well as at any point during a digital session. Contextual access applies fine-grained authorization policies, adaptive risk, multi-factor authentication, and push authorization, yet only requires these stronger authentication mechanisms when necessary to make it easier for users while maintaining system security.
Next Generation AuthX (Authentication and Authorization)	Traditional authentication and authorization methods include usernames and passwords, as well as third-party validated data elements, such as social security numbers and birthdates. However, in a Zero Trust model, it is assumed that these authenticators may be compromised. Therefore, digital identity providers should offer Next Generation AuthX consisting of continuous assessment for authorization and authentication. This includes transactional authorization and authentication, which requires users to perform actions and provide additional factors, often multiple times, for each high-risk transaction within a session. Authentication trees are an integral part of Next Gen AuthX. As a visual, drag and drop workflow, authentication trees allow administrators to easily configure, measure, and adjust login journeys using digital signals including device, contextual, behavioral, user choice, analytics, and risk-based factors. With an intuitive drag-and drop interface, administrators can also quickly consume out-of-the box authenticators, utilize existing authenticators, and integrate with cyber security solutions.
Log In Analytics and Decision Logic	The only way to continuously improve and secure the customer journey is to have data-driven insight. As part of Next Generation AuthX, user login analytics offer metrics and timers that analyze end-user interactions and their devices across all channels and lines of business. Digital identity platforms should therefore be able to monitor performance of third party fraud and analysis services that impact login journeys. Platforms should also allow administrators to optimize the customer journey with contextual and behavioral analytics that investigate what devices and browsers people use, where people log in from, the length of login journeys across the user population, and more. From this, organizations can discover correlations between existing login methods to improve customer adoption rates.
Progressive Profiling	Rather than asking users to fill out extensive registration forms, identity administrators can implement progressive profiling, a technique to collect user information as users interact with the system, on a website or application. For example, organizations can collect just the user's name, email, and password on initial signup. At a later point in time, the user's company and title may be requested.
System Integrations	Identity platforms are an important part of a solution ecosystem that store customer identities and perform data collection and analytics. This ecosystem includes Identity and Access Management (IAM), Mobile Device Management (MDM) systems, Customer Relationship Management (CRM) systems, and marketing automation systems. Unfortunately, most of these ecosystems result in fragmented views of the customer. Advanced digital identity platforms have the ability to integrate and connect with the systems listed above to create a single view of the customer organization-wide. This aggregated data provides a much more robust data-set with which to engage customers, such as using location data from the security system and using it for more customized marketing.

Strategic Component	Description
Privacy by Design and Consent Mechanisms	GDPR mandates that users have control over their personal data, including privacy, security, and usage preferences. For global and regional compliance, it is imperative that digital identity platforms include Privacy by Design and Consent mechanisms based on the UMA 2.0 standard as well as integrate with other software that help meet regulatory requirements. Such mechanisms provide users with fine-grained controls to share and audit data about themselves, their devices and 'things'. A Consent Receipt feature to track user consent is also mandatory for a compliance-ready digital identity platform. Importantly, the user interface of the privacy and control mechanism should be intuitive and friendly.
Data Residency	Data residency and data sovereignty are related concepts covering the legalities of where user data resides, and the legal authority over the data, regardless of where it resides. Generally, data residency requires that a citizen's personal data be collected, stored, and processed only within their country's borders. To address the GDPR concept of data residency, digital identity providers should enable privacy-bound user data storage and fractional replication of personal data. This allows the processing of user data that is context-sensitive to a particular jurisdiction.
Data Aggregation of People, Things, and Their Relationships	To create secure, personalized, omnichannel experiences, digital identity providers must allow organizations to aggregate relational data between people and their 'things' to create a highly comprehensive, single view of the customer. This is achieved by meeting several technical requirements, including establishing a common customer data model, connecting a broad range of data sources, implementing simple synchronization and reconciliation logic, and allowing access to customer data in an appropriate format. Importantly, with billions of digital relationships to support and manage, the most future-looking digital identity providers are developing Identity Graph Engines. These relationship-focused engines represent and query complex and interconnected webs of identity relationships that cross organizations, systems, people, services, devices, business agreements, and more.
Identity at the Edge	As discussed earlier, most IoT 'things' are not secure. Identity at the Edge secures devices and the data they collect with Edge Controllers and Identity Message Brokers. Edge Controllers secure IoT identities and their associated credentials in order to be trusted and usable across numerous connected ecosystems to prevent man-in-the-middle and other types of attacks. Many IoT 'things' use non-secure protocols such as MQTT to identify themselves and send and receive information. Identity Message Brokers secure such protocols by translating MQTT, and other protocols, to HTTPS and making authentication and authorization for the devices and data possible.
API First Model	The API First Model is a developer-centric method of creating a solution. Within this model, a provider first creates the API and then builds the platform around it. This results in less complexity for external developers and organizations. For ease of use, scalability, and flexibility, digital identity providers should apply this API first development model to create one common REST API framework across the entire platform to provide a single, common method to invoke any identity service. The result should be a simple and secure way to extend identity to all realms, including social, mobile, cloud, and IoT.
Legacy App Support	Most organizations contain a great number of legacy systems and applications. Many of these store customer data and credentials, yet have limited or no built-in capabilities for user registration, authentication, authorization, or federation. Therefore, the ability to connect and extend to legacy systems and apps with a contemporary identity system is an important feature of digital identity platforms. This is done through an Identity Gateway, which allows both legacy and contemporary systems and applications to talk to one another fluidly and securely.
DevOps Friendly Architecture and Micro-services	DevOps enables software development and deployment to run in a continuous cycle, allowing organizations to rollout new capabilities faster by reducing time to production. Digital identity providers should provide a DevOps friendly architecture with the ability to leverage DevOps tools, such as automating and orchestrating push-button deployment and continuous delivery. They should also use containerized images for rapid automation, with Docker support, as well as have an intelligent architecture that separates configuration from binaries to easily leverage version control for DevOps artifacts. Additionally, digital identity providers should provide command-line tools for remote configuration. Microservices is another important development method that focuses on building and deploying applications as groups of modular, composable services within an application. The benefit of microservices is the ability to singularly modify a service without impacting the others.

Strategic Component	Description
Serverless Architecture and Patterns	As discussed in the Availability and Scale section, organizations need to account for a variety of scale scenarios, such as millions of concurrent and simultaneous sessions. To do this cost effectively, leading digital identity providers support Serverless Architecture Patterns. Serverless Architecture allows servers to not only spin up and down as needed, but for data-center leasing terms to be based on the size of memory used on a server as well as the length of time that it was used. This method eliminates the need for developers to manage large quantities of servers that are only used periodically for peak load times.
Multi-Cloud and Hybrid-Cloud Support	Multi-cloud environments have become a recent trend due to their increased flexibility, availability, and scalability. These environments allow organizations to eliminate vendor lock-in and speed time-to-market while reducing complexity and saving time and money. Hybrid environments include both on-premise and cloud environments. Cloud environments support needs at scale, while on-premises environments are advised to store sensitive data for better security. The advantage of hybrid environments is the flexibility to support any deployment, anywhere, at any time.
Identity Platform as a Service (PaaS)	Maintaining and upgrading identity solutions is complex and labor intensive. With a true identity platform as a service (Identity PaaS), organizations can consume a comprehensive identity platform offering without having to be responsible for things such as hosting, maintenance, upgrades, and more. Further, when the Identity PaaS uses the same code base as the software version, organizations gain the flexibility to consume and deploy identity solutions throughout the enterprise as needed and at scale. These benefits and more allow IT resources to focus on other important initiatives, such as innovation and modernization.
System Auditing and Analytics	System auditing and analytics capabilities are mission-critical functions. Digital identity platform must be able to conduct audits for system security, troubleshooting, usage analytics and regulatory compliance. They should also support a wide range of monitoring and logging capabilities. Audit logs ought to gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. Additionally, digital identity platforms must provide auditing and analytics for the systems they work with, such as partner systems.
Strong Partner Ecosystem	To address the six trends and more, the strongest digital identity solutions are those that work well with a wide variety of other technologies, software, and industry leaders in order to solve the unique goals of each organization. As such, digital identity providers must have a strong ecosystem of respected consultancy, technology, and integrations partners. Further, this partner ecosystem should be designed to immediately and easily support today's needs, as well as be a source of collaboration and innovation for the future.

For more information on strategically supporting the six trends' customer use cases and why traditional systems fall short, read *Evaluating Digital Identity Management Providers for Customer Identity and Access Management: Top Criteria, Differentiators, and Questions to Ask Providers.*

Comparing Digital Identity Management Providers: RFP Questions by Component

Digital identity platforms vary in their components and capabilities. To support the six global trends, the following are critical questions to ask Digital Identity management providers by component for customer use cases.

How does each provider being evaluated answer the critical questions? For each provider, copy the blank RFP question tables below and fill in the answer boxes. ForgeRock's answers are provided in the addendum at the end of this paper. For additional questions by industry, read the industry-specific workbooks.

Basic Component	Questions for Digital Identity and CIAM Providers	Answers
Federated SSO	› Does the provider offer federated single sign-on based on open standards such as OAuth, WS-Federation, WS-Trust, OIDC and SAML?	
Social Registration and Authentication	› Does the provider offer social registration and authentication? › Which social networking services are included in their offering?	
Multi-Factor Authentication	› Does the provider offer multi-factor authentication? › What authentication mechanisms do they offer?	
Authorization	› What types of authorization methods and access controls are offered by the provider?	
Self-Service	› Does the provider offer self-service? › What self-service capabilities does the provider support?	
Identity Store	› Does the solution's identity store encrypt data both at rest and in transit? › Does the solution offer fractional and multi-master replication? › Can the identity store scale to support data from hundreds to millions of identities, including devices and 'things'? › Does the solution's identity store comply with LDAP v3 and integrate seamlessly with any directory?	
Support for a Single View of Identities	› Can the solution integrate with other systems in order to consolidate identity data silos to create a single view of the customer organization-wide? › Can the solution provide live bidirectional synchronization and reconciliation of identity attributes between data stores?	

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Availability at Scale	› Does the solution scale elastically? For example, does it have the ability to scale the identity registration, authentication, and authorization service by many orders of magnitude to respond to predicted peaks, such as during a high profile event, or unpredicted events such as trending content demand or social media activities?	
Open Standards Support	› Does the solution support both basic and advanced open standards, such as OAuth2, OpenID Connect, SAML, UMA 2.0, OAuth2 Device Flow and OAuth 2.0 Proof-of-Possession?	
Zero Trust Security	› Does the solution provide a Zero Trust Security and CARTA model of risk and/or value-based authentication (Adaptive Authentication), enabling people, devices, things, and applications to have different levels of credentials to authenticate against a common Identity store?	

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Distributed Scope Design with Lease Priviledged Access	› Can the solution enable the principle of 'least privileged access' to only grant access that is essential to perform an intended purpose?	
Contextual Access	› Does the solution leverage contextual authentication and authorization factors at any point during a session to assess risk --- invoking stronger authentication mechanisms only when necessary by evaluating who the user is and their context?	
Next Generation AuthX (Authentication and Authorization)	› Can the solution easily configure, measure, and adjust authentication journeys using factors and digital signals (context, risk, behavior, choice, analytics) to not only determine risk, but to improve the user experience and inform downstream apps of the accumulated knowledge gained during the authentication journey? › Does the solution pre-identify a user's digital signal such as location, IP address, device type, operating system, browser type, and more before a username is even collected? › Does the solution provide OOB authenticators, the ability to custom build authenticators, and have rapid integration with third-party authentication, fraud, and risk providers in a centralized place? › Does the solution allow authorization and authentication workflows to be easily viewed, created, and changed with drag and drop functionality through workflows and trees? › Does the solution include transactional authorization for high-risk transactions within a session?	
Log In Analytics and Decision Logic	› Does the solution evaluate whether logins result in increased abandoned shopping carts? › Does the solution assess average time for call-outs to fraud systems? › Does the solution monitor performance of Service Level Agreements that impact login journeys? › Does the solution determine if shorter login journeys result in fewer help desk calls?	
Progressive Profiling	› Does the solution support progressive profiling across the customer journey and lifecycle?	
System Integrations	› For greater personalization and an omnichannel experience, does the solution integrate with other systems and enable the consolidation of multiple identity silos to create a single view of the customer organization-wide?	
Privacy by Design by Consent Mechanisms	› Does the solution support a privacy and consent framework based on the UMA 2.0 standard? › Can the solution provide users with fine-grained controls to share and audit data about themselves, their devices and 'things'? › Does the solution include a Consent Receipt feature? › Does the solution support "the right to be forgotten" that adheres to regulations such as GDPR?	
Data Residency	› Does the solution support data residency?	
Data Aggregation of People, Things, and Their Relationships	› Does the solution include identity relationship modelling at a granular level (parents, children, friends, and so on) for identity management between those relationships?	
Identity at the Edge	› Does the solution use Edge Controllers to secure IoT identities and their associated credentials in order to be trusted and usable across numerous connected ecosystems to prevent man-in-the-middle and other types of attacks?	
API First Model	› Does the provider use an API first development model to create one common REST API framework across the entire platform to provide a single, common method to invoke any identity service?	

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Legacy App Support	› Does the solution have the ability to connect and extend to legacy systems and apps through an Identity Gateway?	
DevOps Friendly Architecture and Micro-services	› Does the solution support modern deployment DevOps approaches with containerization and orchestration technologies such as Docker and Kubernetes? › Is the solution built within a microservices architecture?	
Serverless Architecture Patterns	› Does the solution support serverless architecture patterns? › Does the solution support three-tier web application pattern (REST), ETL (extract, transform, load) patterns, and automation and deployment patterns (such as CI/CD)?	
Multi-Cloud and Hybird-Cloud Support	› Can the solution be deployed within any cloud environment, including multi-cloud, bring-your-own-cloud, or hybrid cloud, within minutes for millions of identities?	
Identity Platform as a Service (PaaS)	› Does the provider offer their entire identity platform as a service (PaaS)? › Do the provider's as-a-service and software offerings have feature parity?	
System Auditing and Analytics	› Is the solution able to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance? › Can the solution also support a wide range of monitoring and logging capabilities?	
Strong Partner Ecosystem	› Does the provider have a strong ecosystem of respected consultancy, technology, and integrations partners?	

Comparing Digital Identity Management Providers: Components Matrix

Each of the digital identity strategic components is integral to meet all of the six global trends. Again, going beyond the identity basics is a necessity for today's use cases as well as what's to come. **Do each of the providers being evaluated cover all of the strategic components? Check the boxes accordingly.**

	Personalized experiences and deliver omnichannel experiences	Secure and connect billions of customer and IoT identities and data	Authenticate and authorize billions of logins and transactions daily	Facilitate security, analytics, privacy, and control	Support and adhere to regulations (GDPR, HIPAA, Open Banking, PSDII)	Integrate with other systems	Easily scale to meet demands and requirements	Identify and protect against fraudulent or malicious activities	Provider 1: ForgeRock	Provider 2:	Provider 3:	Provider 4:	Provider 5:
Federated SSO	✔	✔	✔			✔	✔	✔	✔				
Social Registration and Authentication	✔	✔	✔	✔		✔	✔		✔				
Multi-Factor Authentication		✔	✔	✔	✔			✔	✔				
Authorization		✔	✔	✔	✔		✔	✔	✔				

	Personalized experiences and deliver omnichannel experiences	Secure and connect billions of customer and IoT identities and data	Authenticate and authorize billions of logins and transactions daily	Facilitate security, analytics, privacy, and control	Support and adhere to regulations (GDPR, HIPAA, Open Banking, PSDII)	Integrate with other systems	Easily scale to meet demands and requirements	Identify and protect against fraudulent or malicious activities	Provider 1: ForgeRock	Provider 2:	Provider 3:	Provider 4:	Provider 5:
Self-Service	✔			✔	✔		✔		✔				
Identity Store	✔	✔		✔	✔	✔	✔	✔	✔				
Support for a Single View of Identities	✔	✔	✔	✔	✔	✔	✔	✔	✔				
DevOps Friendly	✔						✔		✔				
Availability at Scale	✔	✔	✔	✔	✔	✔	✔	✔	✔				
Open Standards Support							✔		✔				
Zero Trust Security			✔	✔		✔		✔	✔				
Distributed Scope Design with Lease Priviledged Access			✔	✔	✔			✔	✔				
Contextual Access	✔	✔	✔	✔	✔	✔		✔	✔				
Next Generation AuthX (Authentication and Authorization)	✔	✔	✔	✔	✔	✔	✔	✔	✔				
Log In Analytics and Decision Logic	✔	✔	✔	✔		✔	✔	✔	✔				
Progressive Profiling	✔			✔		✔	✔		✔				
System Integrations	✔				✔	✔			✔				
Privacy by Design by Consent Mechanisms	✔			✔	✔				✔				
Data Residency	✔			✔	✔				✔				
Data Aggregation of People, Things, and Their Relationships	✔						✔		✔				
Identity at the Edge	✔	✔	✔	✔				✔	✔				
API First Model	✔				✔		✔		✔				
Legacy App Support	✔						✔		✔				

	Personalized experiences and deliver omnichannel experiences	Secure and connect billions of customer and IoT identities and data	Authenticate and authorize billions of logins and transactions daily	Facilitate security, analytics, privacy, and control	Support and adhere to regulations (GDPR, HIPAA, Open Banking, PSDII)	Integrate with other systems	Easily scale to meet demands and requirements	Identify and protect against fraudulent or malicious activities	Provider 1: ForgeRock	Provider 2:	Provider 3:	Provider 4:	Provider 5:
DevOps Friendly Architecture and Micro-services	✔	✔	✔	✔		✔	✔	✔	✔				
Serverless Architecture Patterns							✔		✔				
Multi-Cloud and Hybird-Cloud Support							✔		✔				
Identity Platform as a Service (PaaS)	✔	✔	✔	✔	✔	✔	✔	✔	✔				
System Auditing and Analytics				✔	✔				✔				
Strong Partner Ecosystem					✔		✔		✔				

ForgeRock: One Comprehensive Yet Simple Solution for Every Use Case

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.

A leader and visionary for a reason, the ForgeRock Identity Platform is the only solution future-minded and designed to support the six global trends, secure the enterprise, build customer trust and loyalty, and grow business opportunities and revenue today and well into the future.

For more information, read:

- *The Top Six Global Trends Shaping Business and Society: Why Digital Identity Is the New Imperative for Customer Identity and Access Management*
- *Evaluating Digital Identity Management Providers for Customer Identity and Access Management: Top Criteria, Differentiators, and Questions to Ask Providers*

Ready to Get Started? Contact Us

To get started, contact us and learn how ForgeRock can help your organization.

Addendum: ForgeRock Answers to the RFP Questions by Component

Basic Component	Questions for Digital Identity and CIAM Providers	Answers
Federated SSO	› Does the provider offer federated single sign-on based on open standards such as OAuth, WS-Federation, WS-Trust, OIDC and SAML?	Yes. The ForgeRock Identity Platform is comprised of a number of standards-based components, built on a common framework using best in class open technologies. ForgeRock contributes to many of these standards to ensure they continue to develop and retain relevancy as technology and requirements evolve. ForgeRock sees open standards as vital to ensuring compatibility and interoperability with external systems, guarding against obsolescence, providing choice, and avoiding vendor lock in.
Social Registration and Authentication	› Does the provider offer social registration and authentication? › Which social networking services are included in their offering?	Yes. The ForgeRock Identity Platform provides native support for social registration, allowing users to register new accounts using information from social identity providers including Google, Facebook, LinkedIn, Amazon, and many others. You can set up any custom social identity provider, as long as they are fully compliant with the OAuth 2.0 authorization framework or OIDC standards. The ForgeRock platform also supports delegated authentication through third-party social identity providers, such as Facebook, Google, and VKontakte.
Multi-Factor Authentication	› Does the provider offer multi-factor authentication? › What authentication mechanisms do they offer?	Yes. Multi-Factor Authentication can be implemented by configuring an authentication tree with authentication nodes from different categories of authentication. The ForgeRock Identity Platform includes a wide range of built-in authentication nodes. Additional node types are also provided on the ForgeRock Marketplace.
Authorization	› What types of authorization methods and access controls are offered by the provider?	The ForgeRock Identity Platform supports course and fine-grained contextual, continuous, and transactional authorization. The platform also supports all common forms of access control: Role Based Access Control (RBAC), Attribute Based Access Control (ABAC), Policy Based Access Control (PBAC), Risk-Adaptable Access Controls (RAdAC) and Relationship Based Access Control (RelBAC).
Self-Service	› Does the provider offer self-service? › What self-service capabilities does the provider support?	Yes. The ForgeRock Identity platform provides comprehensive user self-service capabilities that include user registration or sign-up, forgotten password reset and username retrieval. This is supported by a fully brandable and customizable user interface (UI) but is also available via a REST API service which allows the services to be integrated into an existing or custom site.
Identity Store	› Does the solution's identity store encrypt data both at rest and in transit? › Does the solution offer fractional and multi-master replication? › Can the identity store scale to support data from hundreds to millions of identities, including devices and 'things'? › Does the solution's identity store comply with LDAP v3 and integrate seamlessly with any directory?	Yes. The ForgeRock Identity Platform supports Transport Layer Security (TLS)/Secure Sockets Layer (SSL) encryption to ensure data is encrypted during transit. The primary data store for ForgeRock Access Management is ForgeRock Directory Services, which implements both hashing and encryption of fields containing password information. Passwords are by default stored in ForgeRock Directory Services as salted and hashed values. In addition the entire data storage backend can be encrypted.

Basic Component	Questions for Digital Identity and CIAM Providers	Answers
Support for a Single View of Identities	› Can the solution integrate with other systems in order to consolidate identity data silos to create a single view of the customer organization-wide? › Can the solution provide live bidirectional synchronization and reconciliation of identity attributes between data stores?	Yes. The ForgeRock Identity Platform enables you to build a single view of the user in order to gain a complete picture of your customers and their interactions with your organization. This can be achieved by meeting several requirements, including establishing a common customer data model, connecting a broad range of data sources, implementing simple synchronization and reconciliation logic, and allowing access to customer data in an appropriate format. Reconciliation is the process of bidirectional synchronization of objects between different data stores. The reconciliation of data is one of the core features of the ForgeRock Identity Management solution. As long as a connector is available to access data in an application, reconciliation can be configured and customized to meet your requirements. ForgeRock Identity Management can be used as either the source or the target, or neither.

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Availability and Scale	› Does the solution scale elastically? For example, does it have the ability to scale the identity registration, authentication, and authorization service by many orders of magnitude to respond to predicted peaks, such as during a high profile event, or unpredicted events such as trending content demand or social media activities?	Yes. The ForgeRock Identity Platform was designed from the ground up to provide telco-grade scalability and availability. By adhering to open standards, modular architecture, and best practice design principles, ForgeRock products have proven to be extremely robust, lightweight and highly scalable, and simple to deploy in highly-available environments spanning multiple data centers, hosting platforms, and geographies. Many ForgeRock customers use automated deployment approaches in physical or virtually hosted environments with great success. Further, with a clear industry trend towards a complete 360 DevOps approach that utilizes containerization and orchestration, ForgeRock includes support for the industry leading Kubernetes orchestration engine and Docker containerization.
Open Standards Support	› Does the solution support both basic and advanced open standards, such as OAuth2, OpenID Connect, SAML, UMA 2.0, OAuth2 Device Flow and OAuth 2.0 Proof-of-Possession?	Yes. The ForgeRock Identity Platform supports all major federation and authorization standards, including SAML 2.0, WS-Federation, OAuth 2.0, OpenID Connect, User Managed Access (UMA), OAuth2 Device Flow and OAuth 2.0 Proof-of-Possession. Applications which have federation capabilities, both on-premises and cloud-hosted, integrate seamlessly with ForgeRock Access Management. ForgeRock is also a GSMA Mobile Connect (MC) Vendor allowing you to provide MC services to your customers and ecosystem partners.
Zero Trust Security	› Does the solution provide a Zero Trust Security and CARTA model of risk and/or value-based authentication (Adaptive Authentication), enabling people, devices, things, and applications to have different levels of credentials to authenticate against a common Identity store?	Yes. ForgeRock understands that in a world where security breaches are commonplace and insiders pose the greatest threat to enterprises, authentication and authorization must be continuous. Our standards-based, open platform combined with Intelligent Access and a variety of policy enforcement options allows companies to make continuous security decisions of employees and partners making ForgeRock the ideal solution for organizations making strategic bets around Zero Trust or CARTA security models and cloud native architectures. 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.

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Distributed Scope Design with Lease Priviledged Access	› Can the solution enable the principle of 'least privileged access' to only grant access that is essential to perform an intended purpose?	Yes. The ForgeRock Identity Platform supports 'least privileged access'. For example, customers are only permitted to access the exact information and resources necessary for a particular and legitimate purpose. ForgeRock also delivers this through fine-grained authorization, a mechanism to 'distribute' and assign strongly-typed scopes to applications, API endpoints, and other protected resources. Scopes are coupled with real-time context at policy-enforcing gates throughout the identity ecosystem. Scopes for fine-grained, actionable rules that can be used to make authorization decisions are also applied.
Contextual Access	› Does the solution leverage contextual authentication and authorization factors at any point during a session to assess risk --- invoking stronger authentication mechanisms only when necessary by evaluating who the user is and their context?	Yes. Contextual authorization (also known as continuous authorization or continuous authentication) is supported in the ForgeRock Identity Platform through the use of authentication levels and authorization policies. With ForgeRock Intelligent Access, 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.
Next Generation AuthX (Authentication and Authorization)	› Can the solution easily configure, measure, and adjust authentication journeys using factors and digital signals (context, risk, behavior, choice, analytics) to not only determine risk, but to improve the user experience and inform downstream apps of the accumulated knowledge gained during the authentication journey? › Does the solution pre-identify a user's digital signal such as location, IP address, device type, operating system, browser type, and more before a username is even collected? › Does the solution provide OOB authenticators, the ability to custom build authenticators, and have rapid integration with third-party authentication, fraud, and risk providers in a centralized place? › Does the solution allow authorization and authentication workflows to be easily viewed, created, and changed with drag and drop functionality through workflows and trees? › Does the solution include transactional authorization for high-risk transactions within a session?	Yes. With ForgeRock Intelligent Access, workflow-like decision trees can be easily viewed, created, changed, and configured with drag and drop functionality 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. Extensibility is a key feature of the ForgeRock Identity Platform. Customer specific authentication methods can be easily added using scripting that can be configured in the same way as out-of-the-box authentication methods. ForgeRock also has an extensive community and partner network that provides additional authentication methods. It does not matter which vendor provides the additional authentication methods as long as standards based integration endpoints or APIs are available that the ForgeRock platform can invoke to trigger and validate authentication events. Common authenticators include: › Third-party authentication nodes: ForgeRock has a rapidly growing community of technology partners who are contributing authentication nodes via the ForgeRock Marketplace. These nodes enable various best-of-breed, strong authentication, risk-assessment and service providers to be incorporated into the authentication flow. › Custom authentication nodes: Organizations can easily author their own authentication nodes and incorporate them into their deployment. Where the node functionality is lightweight, it may be an option to script the out-of-the-box decision node in Groovy or JavaScript to perform REST calls to other authentication factors for example. The ForgeRock Identity Platform supports transactional authorization to improve security by requiring a user to perform additional authentication action(s) when trying to access a resource protected by an authorization policy. While transactional authorization can make use of any authentication method, typically organizations would use ForgeRock Push Authenticator to send a push notification to a user's mobile device to authorize access to a protected resource.

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Log In Analytics and Decision Logic	› Does the solution evaluate whether logins result in increased abandoned shopping carts? › Does the solution assess average time for call-outs to fraud systems? › Does the solution monitor performance of Service Level Agreements that impact login journeys? › Does the solution determine if shorter login journeys result in fewer help desk calls?	Yes. The ForgeRock Identity Platform provides usage analytics which can help provide data for meeting service level agreements, measuring performance, and gaining greater insight into how end users and their devices interact with applications and services. Usage analytics can occur at many different points during a user's interaction with a service. With ForgeRock Intelligent Access, many different contextual signals may be used during a customer login, to control and adapt the authentication journey, establish the level of assurance or risk from the authentication, and also to gather useful data about the authentication. For example, login journeys may make use of the customer's geolocation, perhaps to detect fraudulent activity, or provide a more seamless experience. The same information can be provided to downstream applications and APIs, or stored or forwarded for analytics. ForgeRock Intelligent Access provides specific metrics gathering nodes for this purpose, as well as timer nodes which record the time taken between authentication steps. These are often used to establish authentication patterns; the percentage of users who are logging in from mobile devices vs desktops, or Apple phones vs Android devices, geographies, networks, times of day, etc. Information gathered by timer nodes can be used to ensure that login failure rates are below accepted limits, and to make sure that a particular authentication journey is not hindering customers.
Progressive Profiling	› Does the solution support progressive profiling across the customer journey and lifecycle?	Yes. The ForgeRock Identity Platform includes a progressive profiling capability. This allows organizations to defer requesting additional details from the customer to a time when it is needed.
System Integrations	› For greater personalization and an omnichannel experience, does the solution integrate with other systems and enable the consolidation of multiple identity silos to create a single view of the customer organization-wide?	Yes. The ForgeRock Identity Platform enables you to build a single view of the user, in order to gain a complete picture of your customers and their interactions with your organization. This can be achieved by meeting several requirements including establishing a common customer data model, connecting a broad range of data sources, implementing simple synchronization and reconciliation logic, and allowing access to customer data in an appropriate format.

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Privacy by Design by Consent Mechanisms	› Does the solution support a privacy and consent framework based on the UMA 2.0 standard? › Can the solution provide users with fine-grained controls to share and audit data about themselves, their devices and 'things'? › Does the solution include a Consent Receipt feature? › Does the solution support "the right to be forgotten" that adheres to regulations such as GDPR?	Yes. ForgeRock User-Managed Access (UMA) is a privacy and consent solution based on UMA 2.0 that helps address compliance with consent requirements of privacy laws. Through 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 user 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 to Terms and Conditions (T&Cs) and privacy notices, at both account registration time and at authentication time, and enables users to manage account information over time. ForgeRock is a member of the board of the Kantara Initiative, with the goal of providing more clarity and an industry-developed common practices guideline document around consent and privacy policies for use by organizations that manage and use large amounts of identity information and data. The Kantara Initiative has developed a consent receipt specification, based on current privacy and data protection principles as set out in various data protection laws, regulations and international standards. A Consent Receipt is record of authority granted by a Personally Identifiable Information (PII) Principal to a PII Controller for processing of the Principal's PII. The record of consent is human-readable and can be represented as standard JSON. ForgeRock fully supports the implementation of the Kantara consent receipt specification to capture all details of a PII collection or update activity. Any creation or modification of a customer consent, regardless of source channel or process, can trigger the server-side generation of a consent receipt, which includes information about the PII collection point, among other properties of the data collection activity.
Data Residency	› Does the solution support data residency?	Yes. Data residency and data sovereignty cover the legalities of where user data resides, and the legal authority over the data, regardless of where it resides. To address data residency, the ForgeRock Identity Platform enables privacy-bound user data storage and fractional replication of personal data. This allows the processing of user data that is context-sensitive to a particular jurisdiction. User data can be provisioned to ForgeRock Directory Services, which acts as a single published endpoint. Behind this endpoint the directory service is responsible for persisting either all or parts of an identity object across various instances of directory services, through fractional replication. In addition to fractional replication, Forgerock also supports multimaster replication, master-slave replicatication and subtree replication.
Data Aggregation of People, Things, and Their Relationships	› Does the solution include identity relationship modelling at a granular level (parents, children, friends, and so on) for identity management between those relationships?	Yes, the ForgeRock Identity Platform can be used to model relationships between multiple different identities.

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Identity at the Edge	› Does the solution use Edge Controllers to secure IoT identities and their associated credentials in order to be trusted and usable across numerous connected ecosystems to prevent man-in-the-middle and other types of attacks?	Yes. ForgeRock Edge Security offers complete end-to-end security for IoT deployments. Further, 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. Core capabilities of the ForgeRock Identity Platform to support IoT initiatives include: a common REST API, standards support, OAuth 2.0 device flow, Proof of Possession support, IoT broker integration, stateless architecture for IoT scale, a managed object model, and an IoT-ready policy engine.
API First Model	› Does the provider use an API first development model to create one common REST API framework across the entire platform to provide a single, common method to invoke any identity service?	Yes. One of the unique features of the ForgeRock Identity Platform is that all components of the platform share a single, easy to use RESTful web API, known as ForgeRock common REST API (CREST). This common API makes it easy for implementers and deployers of the ForgeRock Identity platform to solve business-critical identity management related problems quickly, avoiding the need for developers to learn more complex JAVA APIs.
Legacy App Support	› Does the solution have the ability to connect and extend to legacy systems and apps through an Identity Gateway?	Yes. Legacy applications, or applications which simply require protection from unauthenticated access but have little interest in the identity of the user, may only require light-touch integration or zero-touch integration through the use of ForgeRock Identity Gateway.
DevOps Friendly Architecture and Micro-services	› Does the solution support modern deployment DevOps approaches with containerisation and orchestration technologies such as Docker and Kubernetes? › Is the solution built within a microservices architecture?	Yes. The ForgeRock Identity Platform can be deployed using DevOps techniques including containerization and orchestration. Deployment in a containerized environment is demonstrated through ForgeRock DevOps examples, which include scripts and descriptor files that enable you to build reference Docker images for the ForgeRock platform. Orchestration is demonstrated through sample Kubernetes manifests that can be adapted to your own environments. ForgeRock also delivers a Cloud Deployment Model (CDM) that demonstrates a common use ForgeRock Identity Platform architecture installed in a DevOps environment. Using the CDM artifacts and cookbook instructions provided by ForgeRock, you can quickly get the ForgeRock platform running in a Kubernetes cloud environment such as Google GKE or Amazon EKS. The CDM can be used to validate your pre-production deployment against the benchmark results, and you can then customize or scale your deployment environment to meet your specific business requirements. For example ForgeRock Dockerfiles, Helm charts, Kubernetes manifests, utility scripts for deploying DevOps examples, and CDM deployment artifacts, are publicly available in a Git repository (forgeops repository). Creating value through your CIAM architecture means bridging the gaps between the growing number of business applications, APIs, and microservices.The ForgeRock Identity Platform integrates and secures web applications, APIs, and microservices. For example, ForgeRock Identity Gateway in conjunction with ForgeRock Access Management integrates web applications without the need to modify the target application or the container that it runs in - which ultimately delivers significant cost-savings.

Strategic Component	Questions for Digital Identity and CIAM Providers	Answers
Serverless Architecture and Patterns	› Does the solution support serverless architecture patterns? › Does the solution support three-tier web application pattern (REST), ETL (extract, transform, load) patterns, and Automation and deployment patterns (such as CI/CD)?	Yes. ForgeRock supports a variety of scale scenarios, such as millions of concurrent and simultaneous sessions. To do this cost effectively, ForgeRock supports Serverless Architecture Patterns. Serverless Architecture allows servers to not only spin up and down as needed, but for data-center leasing terms to be based on the size of memory used on a server as well as the length of time that it was used. This method eliminates the need for developers to manage large quantities of servers that are only used periodically for peak load times. ForgeRock also supports three-tier web application pattern (REST, GraphQL), ETL (extract, transform, load) patterns such as FanOut and Automation and deployment patterns (such as CI/CD).
Multi-Cloud and Hybrid-Cloud Support	› Can the solution be deployed within any cloud environment, including multi-cloud, bring-your-own-cloud, or hybrid cloud, within minutes for millions of identities?	Yes. The ForgeRock Identity Platform deploys on any cloud (including bring-your-own-cloud, hybrid-cloud, and multi-cloud models) in minutes with preconfigured cloud installation packages of 1M, 10M, and 100M identities.
Identity Platform as a Service (PaaS)	› Does the provider offer their entire identity platform as a service (PaaS)? › Do the provider's as-a-service and software offerings have feature parity?	Yes. ForgeRock 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. Further, ForgeRock's PaaS and software offerings share feature parity.
System Auditing and Analytics	› Is the solution able to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance? › Can the solution also support a wide range of monitoring and logging capabilities?	Yes. The ForgeRock Identity Platform implements a REST-based Audit Logging Service across all of its components, which captures all auditing events critical for system security, troubleshooting, usage analytics and regulatory compliance. This data may be viewed directly or for convenience and reporting purposes, pushed to an external database, Elasticsearch, syslog or SIEM. The ForgeRock Identity Platform provides a variety of standard mechanisms for monitoring and alerting. The platform uses Dropwizard's Metrics as its common metrics framework for adding monitoring capabilities to an application. It includes native support for monitoring component metrics using Prometheus and visualizing this information using Grafana.
Strong Partner Ecosystem	› Does the provider have a strong ecosystem of respected consultancy, technology, and integrations partners?	Yes. The ForgeRock Trust Network unifies ForgeRock's extensive community of technology partners for customers to seamlessly integrate complementary technologies and realize the highest value from their ForgeRock Identity investments. The program establishes a marketplace where customers can discover third-party identity and access management technologies that are commonly used in conjunction with each other.