ForgeRock

CIAM

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

A Workbook

The provisioning of financial services is evolving in response to restless customer expectations, a watershed in regulation, and the constantly shifting technological landscape. Consumers expect to make use of banking services without friction at any time across all of their different devices while on the move between various locations. At the same time, in a world where the attackers have never been so sophisticated and the threats never so prevalent, many consumers are no longer taking for granted that their data will be well managed and secure. Because of this, regulatory trends such as GDPR and PSD2 are underpinning a revolution in how people can take control of, and benefit from, the consent-based sharing of their financial data with selected parties.

To address these trends and necessities of the future, financial services leaders should carefully compare digital identity management providers for customer identity and access management (CIAM).

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 papers detailing the six digital transformation trends and the components needed for customer identity and access management, as well as future-forecasted use cases.

Use this workbook to compare digital identity management providers specifically for the financial services industry by copying the RFP question tables and filling in the blank answer boxes provided for each provider. ForgeRock answers are included within this workbook.

CIAM Questions to Ask Digital Identity Management Providers: Financial Services Industry

Question	Reason This Is Important To Ask	Answer
Does the solution enable rapid onboarding of customers?	Rapid onboarding is a very simplified processes for customer registration and proofing that enables new customers to be up and running in minutes. Challenger banks like Starling/ Monzo use this type of onboarding.	
How does the solution support existing customers to apply for new services easily?	The ability to recognize customers and provide a single view to pre-populate application forms speeds up the application process and enhances the customer experience.	
Does the solution centrally define and administer authentication and authorization policies in one place for all business units across the entire organization?	Banks often struggle with centrally managing policies that span lines of business and different geographies. By utilizing a single system to define and administer authentication and authorization policies in one place for all business units, an entire organization can serve customers and run their operations and business more accurately and efficiently.	
Does the solution adequately protect personal data stored in a customer identity data store and if so, how? For example, the use of an appropriate encryption algorithm, along with the ability to address cross-border juris-dictional requirements related to data sovereignty.	Data controls have long been a requirement for multinational financial institutions. The bar has been raised with new data laws such as the GDPR and Australia's CDR, which continue to expand requirements for the management of personal data. Adequately protecting personal data stored in a customer identity data store, along with the ability to address cross-border jurisdictional requirements related to data sovereignty, is important to meet such regulations and be prepared for future needs.	

Question	Reason This Is Important To Ask	Answer
Does the solution support "cardholder not present" security flows?	"Cardholder not present" authentication is used where the cardholder does not or cannot physically present a bankcard at the time an order is made or payment affected. Typically these transactions represent a higher level of risk as there is no means to be sure the card owner is actually the person entering the details and making the transaction. Because "cardholder not present" is an important banking use case that comes up frequently, it must be supported by a digital identity platform.	
Does the solution leverage contextual authentication and authorization factors to assess risk — invoking stronger authentication mechanisms only when necessary by evaluating 'who is the user' and 'what is the context'?	Real-time assessment of contextual attributes is essential to deliver security within a paradigm of 'zero trust' (also called a zero trust security model). Real-time assessment of contextual attributes also benefits the customer journey by reducing friction and increasing opportunities for personalization.	
Please describe how the solution can leverage a matrix of 'multi-level' or 'step-up' authentication methods including push authorization, one time passcodes, and biometrics as a response to identified risks or triggers by policy settings.	Step-up authentication is the act of validating a user's identity with a stronger mechanism than the original authentication when the user attempts to access a high-value resource. For example, an online banking application may allow a user to log in with a username and password and carry out a range of transactions. However, it may request a one-time password generated by a hardware device when the user attempts to add a payee to their list of payees. Configuring seamless customer journeys that provide appropriate responses to risk factors is essential to counter fraud within banking services. The ability to manage existing, new, and changing methods of authentication addresses multiple banking requirements.	
Does the solution support all identity, authentication, and fine grained authorization requirements stemming from the PSD2 regulation, Open Banking specification, and KYC/AML requirements with future support for their evolution?	There is an environment of constant and growing regulatory requirements across all banks in Europe and the UK, with other countries following similar design patterns for Open Banking. This makes the support for all identity, authentication, and fine grained authorization a necessity.	
How does the solution support DevOps and a continuous delivery model, utilizing microservices and modern deployment approaches with containerization and orchestration technologies, such as Docker and Kubernetes?	DevOps is increasingly relevant for the digital transformation of Financial Services, using Agile development methods to deploy to both private and public cloud environments.	
Please provide details on how the solution provides authentication across different channels, including but not limited to: › **Mobile** › **Web** › **Contact Centers** › **Branches**	The ability to recognize customers no matter the channel of access to services is essential. By doing so, the appropriate authentication mechanisms can be managed across all channels.	

Question	Reason This Is Important To Ask	Answer
Describe how the solution supports the requirement to allow customers to centrally view and manage the consent they have provided for sharing of their data with any third parties?	Consent is increasingly important for institutions to manage and offer their customers more dynamic control of the information being shared, especially with third parties for the purposes of marketing. This is an important factor in the efforts to be compliant with the GDPR.	
Please describe how the solution defines, collects, and shares metrics across the entire data-management lifecycle (data acquisition, maintenance, distribution, and consumption) etc.	Defining, collecting, and sharing metrics across the entire data-management lifecycle is important in terms of gathering threat and fraud analytics data. While customers are accessing financial services, signals from their behavior can be detected and, if necessary, will trigger significant security responses. Defining, collecting, and sharing metrics across the entire data-management lifecycle can also inform customer experience and aid marketing teams focused on acquisition and growth of services through progressive profiling.	
Future propositions may include some form of delegated control or delegated authentication, such as a parent managing an account on behalf of a child. Please illustrate how the solution could achieve this and allow different levels of access for the parent and child.	Forward-thinking financial institutions recognize that delegating authority is a requirement in many scenarios and supports a focus on ensuring bank loyalty amongst the extended family.	
How capable is the solution for rapid integration with third-party tools?	Between legacy IAM and other security solutions, combined with the deployment of new methods, the ability to provide qualified integrations is a real differentiator between digital identity solutions.	
Please explain the recommended deployment architecture and how the solution supports both horizontal and vertical scalability.	Given the critical nature of banking services and the increasing adoption of cloud-based hosting platforms, it is important to express the ability to not only deploy into hybrid environments, but also to manage growth in customer acquisition and spikes in demand.	

ForgeRock's Answers

Question	Reason This Is Important To Ask	ForgeRock Answer
Does the solution enable rapid onboarding of customers?	Rapid onboarding is a very simplified processes for customer registration and proofing that enables new customers to be up and running in minutes. Challenger banks like Starling/Monzo use this type of onboarding.	Yes, the ForgeRock Identity Platform provides an embedded workflow and business process engine through which you can customize a workflow to enable gathering additional fields to enhance user experience. Login and registration workflows can be customized and configured to include a collection of user data as needed, based on previously supplied data, and additional user preferences or computed heuristics, including out-of-band processing (such as SMS). This can be addressed through a declarative approach that ForgeRock supports for enhancing the user schema.
How does the solution support existing customers to apply for new services easily?	The ability to recognize customers and provide a single view to pre-populate application forms speeds up the application process and enhances the customer experience.	Yes, the ForgeRock Identity Platform ties customers to unique digital identities allowing financial institutions to understand who their customers are, wherever they are. By consolidating the identity data of users, services, and connected things to create a unified customer profile across all digital channels, financial institutions can simplify processes and create convenient customer experiences such as bank-switching and onboarding. Further, ForgeRock's user self-service options enable customers to manage their preferences linked to their unique customer identities across the business.
Does the solution centrally define and administer authentication and authorization policies in one place for all business units across the entire organization?	Banks often struggle with centrally managing policies that span lines of business and different geographies. By utilizing a single system to define and administer authentication and authorization policies in one place for all business units, an entire organization can serve customers and run their operations and business more accurately and efficiently.	Yes, the ForgeRock Identity Platform is designed around the concept of a centralized identity and access management platform, allowing flexible configuration to support many applications at once across an organization. The ForgeRock Identity Platform satisfies the need for multiple configurations for different applications by using either realms, authentication/authorization, or a combination of query parameters when invoking services via the REST API. A realm is a combined set of configurations within ForgeRock Access Management designed for a subset of an organization, but still within a single logical instance. Realms include configuration for applications, authentication modules/chains or nodes/trees, authorization, access policies, and page branding. Typically, customer applications are written to use their own login pages, which use the ForgeRock REST API and will apply their own branding.
Does the solution adequately protect personal data stored in a customer identity data store and if so, how? For example, the use of an appropriate encryption algo-rithm, along with the ability to address cross-border jurisdictional requirements related to data sovereignty.	Data controls have long been a requirement for multinational financial institutions. The bar has been raised with new data laws such as the GDPR and Australia's CDR, which continue to expand requirements for the management of personal data. Adequately protecting personal data stored in a customer identity data store, along with the ability to address cross-border jurisdictional requirements related to data sovereignty, is important to meet such regulations and be prepared for future needs.	To address protecting personal data stored in a customer identity data store and the ability to address cross-border jurisdictional requirements related to data sovereignty, ForgeRock employs both Data in Transit Encryption and Data at Rest Encryption.

Question	Reason This Is Important To Ask	ForgeRock Answer
Does the solution support "cardholder not present" security flows?	"Cardholder not present" authentication is used where the cardholder does not or cannot physically present a bankcard at the time an order is made or payment affected. Typically these transactions represent a higher level of risk as there is no means to be sure the card owner is actually the person entering the details and making the transaction. Because "cardholder not present" is an important banking use case that comes up frequently, it must be supported by a digital identity platform.	Yes, the ForgeRock Identity Platform can enable organizations to secure "cardholder not present" and other similar types of transactions to reduce the risk associated with them through the ForgeRock Identity Gateway, step-up authentication, and transactional authorization. Additionally, ForgeRock's Intelligent Access provides a powerful platform for modeling the authentication journey in an authentication workflow tree, using authentication nodes to detect digital signals.
Does the solution leverage contextual authentication and authorization factors to assess risk — invoking stronger authentication mechanisms only when necessary by evaluating 'who is the user' and 'what is the context'?	Real-time assessment of contextual attributes is essential to deliver security within a paradigm of 'zero trust' (also called a zero trust security model). Real-time assessment of contextual attributes also benefits the customer journey by reducing friction and increasing opportunities for personalization.	Yes, 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.
Please describe how the solution can leverage a matrix of 'multi-level' or 'step-up' authentication methods including push authorization, one time passcodes, and biometrics as a response to identified risks or triggers by policy settings.	Step-up authentication is the act of validating a user's identity with a stronger mechanism than the original authentication when the user attempts to access a high-value resource. For example, an online banking application may allow a user to log in with a username and password and carry out a range of transactions. However, it may request a one-time password generated by a hardware device when the user attempts to add a payee to their list of payees. Configuring seamless customer journeys that provide appropriate responses to risk factors is essential to counter fraud within banking services. The ability to manage existing, new, and changing methods of authentication addresses multiple banking requirements.	Step-up authentication is addressed with ForgeRock's Intelligent Access which includes authentication nodes that can be added to an authentication tree in any position or workflow to either set or modify the authentication level. Controlling access to specific resources is done through authorization rules. ForgeRock Access Management has a policy engine which allows rules to evaluate the current authentication level and trigger step-up authentication if the user needs to access a more sensitive resource. Additionally, transactional authorization may be used in cases where strong authentication is required only to approve a single, atomic transaction, such as a high value payment, or some other approval step. When step-up authentication is used, the authentication level remains at the elevated level until the session is ended, so any subsequent transactions do not require re-authentication. Transactional authorization ensures that the user authenticates every time a secure transaction is performed.

Question	Reason This Is Important To Ask	ForgeRock Answer
Does the solution support all identity, authentication, and fine grained authorization requirements stemming from the PSD2 regulation, Open Banking specification, and KYC/AML requirements with future support for their evolution?	There is an environment of constant and growing regulatory requirements across all banks in Europe and the UK, with other countries following similar design patterns for Open Banking. This makes the support for all identity, authentication, and fine grained authorization a necessity.	Yes, the ForgeRock Identity Platform helps banks with all identity, authentication, and fine grained authorization requirements stemming from the PSD2 regulation, Open Banking specification, and KYC/AML requirements in a number of ways. ForgeRock is part of a select group of identity vendors invited to participate in the Open Banking working group and already provides OAuth 2.0 and OIDC-ready solutions. ForgeRock has also recently launched our own version of the Open Banking Directory to enable third parties to rapidly onboard and test out Open Banking APIs. As an active participant in the development of new industry standards, ForgeRock is positioned for leading-edge implementation of future developments as the transformation of the financial industry continues. ForgeRock has been selected by the Open Banking Implementation Entity (OBIE) to provide a Reference Bank Application, which will be used by leading banks and third-parties to build their own applications in accordance with Open Banking standards. This announcement highlights the completeness of the ForgeRock Identity Platform in solving complex requirements of global enterprises. ForgeRock will deliver the cloud-based application that will drive the demonstration and testing of the Open Banking API ecosystem, much more than just a simple front-end.
How does the solution support DevOps and a continuous delivery model, utilizing microservices and modern deployment approaches with containerization and orchestration technologies, such as Docker and Kubernetes?	DevOps is increasingly relevant for the digital transformation of Financial Services, using Agile development methods to deploy to both private and public cloud environments.	Yes, the ForgeRock Identity Platform is DevOps friendly and supports scriptable CLI and REST interfaces to facilitate automation. The ForgeRock Identity Platform can be deployed today using DevOps techniques including containerization and orchestration. ForgeRock is actively working to develop identity microservices that provide a completely new way of bringing access management services to market. This approach will enable customers to apply leading edge continuous delivery and DevOps patterns to the world of access management.
Please provide details on how the solution provides authentication across different channels, including but not limited to: › **Mobile** › **Web** › **Contact Centers** › **Branches**	The ability to recognize customers no matter the channel of access to services is essential. By doing so, the appropriate authentication mechanisms can be managed across all channels.	Yes, the ForgeRock Identity Platform provides a complete omnichannel security solution for Financial Services covering Mobile, Web, Contact Centers, Branches, as well as other channels such as Open Banking and Automated Assistants (and other new and innovative channels). With the ForgeRock Identity Platform, all customer channel interactions are managed centrally with unified and consistent registration, authentication, authorization and self-service journeys underpinned by ForgeRock's Intelligent Access and a comprehensive single view of the customer (Voice of the Customer). Powered by ForgeRock Identity Management, a single view of the customer is created by integrating, synchronizing, and transforming data from different systems across the organization. All interactions across different touch points in the ForgeRock Identity Platform result in the creation of data covering a wide range of customer activities. All of this data can be securely and automatically exported into existing reporting and monitoring systems. In addition to this, there are numerous hooks and integration points across the platform where events can be generated and data can be exported.

Question	Reason This Is Important To Ask	ForgeRock Answer
Describe how the solution supports the requirement to allow customers to centrally view and manage the consent they have provided for sharing of their data with any third parties?	Consent is increasingly important for institutions to manage and offer their customers more dynamic control of the information being shared, especially with third parties for the purposes of marketing. This is an important factor in the efforts to be compliant with the GDPR.	The ForgeRock Identity Platform offers configurable user registration functionality for self-service account creation and management. This includes a privacy and consent step for the user to confirm they consent to the processing of their data, and enables users to adjust consents over time through the ForgeRock Profile and Privacy Management dashboard. With this functionality, users can withdraw consent after having initially given it, or provide consent after initially having refused it. Privacy and consent management is available to users who register via ForgeRock Identity Management directly or via a social identity provider. User consent can also be collected on authentication during login, for example if the terms and conditions (T&Cs) have changed.
Please describe how the solution defines, collects, and shares metrics across the entire data-management lifecycle (data acquisition, maintenance, distribution, and consumption) etc.	Defining, collecting, and sharing metrics across the entire data-management lifecycle is important in terms of gathering threat and fraud analytics data. While customers are accessing financial services, signals from their behavior can be detected and, if necessary, will trigger significant security responses. Defining, collecting, and sharing metrics across the entire data-management lifecycle can also inform customer experience and aid marketing teams focused on acquisition and growth of services through progressive profiling.	The ForgeRock Identity Platform provides a variety of standard mechanisms for monitoring and alerting in its components. ForgeRock monitoring is designed to allow alerting on the availability and system characteristics of the various platform components, and also on the performance and events that occur for specific functions. The ForgeRock Identity Platform uses Dropwizard's Metrics as its common metrics framework for adding monitoring capabilities to an application. Metrics provide a clean, optimized and easy-to-use API, as well as providing integration with many third-party monitoring frameworks such as Prometheus. All ForgeRock Identity Platform components also share a common audit log service. Audit logs gather operational information about events occurring within a deployment to track processes and security data, such as authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. Audit logs are commonly consumed by third-party SIEM and analytics solutions, such as FireEye®, Guardian Analytics®, Logstash, and Splunk.
Future propositions may include some form of delegated control or delegated authentication, such as a parent managing an account on behalf of a child. Please illustrate how the solution could achieve this and allow different levels of access for the parent and child.	Forward-thinking financial institutions recognize that delegating authority is a requirement in many scenarios and supports a focus on ensuring bank loyalty among the extended family.	With the ForgeRock Identity Platform, delegated access control is supported through the standards OAuth, OpenID Connect (OIDC), and User-Managed Access (UMA). OAuth and OIDC are commonly used to allow a user to delegate permission to a client or application to act on their behalf. This usually includes a set of scopes determining the resources or actions the client is permitted to perform. ForgeRock Access Management acts as an authorization service in this scenario, authenticating the user, recording their consent, and managing the protocol flows required for the OAuth transactions. The protected resource is also responsible for contacting the authorization to confirm the validity and scope of a client's access token. ForgeRock Identity Gateway can also be used to take on this responsibility; for example, to add OAuth/OIDC security to an existing API. The User-Managed Access (UMA) standard provides an extended set of capabilities beyond standard OAuth; for example: a central point of consent management for multiple clients and resources, APIs for the registration of resources, and APIs for registering shares or consent decisions.

Question	Reason This Is Important To Ask	ForgeRock Answer
How capable is the solution for rapid integration with third-party tools?	Between legacy IAM and other security solutions, combined with the deployment of new methods, the ability to provide qualified integrations is a real differentiator between digital identity solutions.	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 framework, known as ForgeRock common REST (CREST), which ships out-of-the-box. CREST defines an API, which is intended for common use across all ForgeRock components and for invoking underlying services across the ForgeRock Identity Platform. It includes a set of easy-to-remember REST calls to Create, Read, Update, Delete, Patch, Action, and Query (CRUDPAQ) identity objects and services. The simplicity of this common API makes it easy for implementers and deployers of the ForgeRock Identity Platform to solve business-critical Identity Management related problems quickly. This avoids the need for developers to learn more complex JAVA APIs. ForgeRock also works with selected technology providers to deliver tightly integrated joint solutions that enhance the ForgeRock Identity Platform and support our customers' digital identity initiatives.
Please explain the recommended deployment architecture and how the solution supports both horizontal and vertical scalability.	Given the critical nature of banking services and the increasing adoption of cloud-based hosting platforms, it is important to express the ability to not only deploy into hybrid environments, but also to manage growth in customer acquisition and spikes in demand.	The ForgeRock Identity Platform is Java-based, threaded, and transactional in nature. As such, it 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. ForgeRock runs benchmark tests across all components of the product suite, routinely using sample user data numbering hundreds of millions of identities. 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 organizations to build reference Docker images for the ForgeRock Identity Platform. Orchestration is demonstrated through sample Kubernetes manifests that can be adapted to an organization's environments.

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 provider by Gartner, the ForgeRock Identity Platform is shaping the future of digital identity management.

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

Learn More About ForgeRock for Your Organization

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