ForgeRock

CIAM

How to Compare Digital Identity Solutions for Internal AM, Citizen CIAM, and FICAM

A Workbook for Government and Public Sector Use Cases

Within the United States, federal and state government agencies are being tasked with several cybersecurity and service-oriented initiatives. Specific to the Federal Government, the Homeland Security Presidential Directive-12 (HSPD-12) is "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. It requires the development and implementation of a government-wide standard for secure and reliable forms of identification for Federal employees and contractors."[1]

In addition to HSPD-12, the White House Office of Management and Budget (OMB) has a government-wide policy to implement identity, credential, and access management (ICAM) to improve access control to logical and physical resources across the Federal Government. Known as FICAM, this initiative aims to "enable the

1 https://www.cio.gov/agenda/cybersecurity/identity-management-hspd-12/

right individual to access the right resource, at the right time, for the right reason."[2] The Office of the Federal Chief Information Officer sums up the required ICAM capabilities as the following:[3]

Further, in May of 2019, new guidance from the White House has been issued to focus identity and access management beyond employees to cover external business partners and citizens. This directive "specifically revises how agencies should conduct identity proofing, establish digital identities and adopt processes for authentication and access control."[4] The White House mandates that "any ICAM capability deployed should be interchangeable, use commercially available products and leverage application programming interfaces to promote interoperability."[5] The White House guidance also includes user privacy and decreasing the number of times users have to disclose privacy data to access government services.

Along with the above, other federal initiatives such as People and Workforce for the 21st Century seek to give agencies the ability to improve both employee and citizen quality of service delivery and customer experience through a modern online experience leveraging the latest technologies. The Office of Management and Budget has also established the US Digital Services Team to help improve government services and customer experience across all agencies. Their goal is to "transform the customer experience by improving the usability and reliability of our Federal Government's most critical digital services; create measurable improvements in customer satisfaction by using the principles and practices proven by leading private sector organizations; increase trust in the Federal Government by improving the experience citizens and businesses have with Federal services whether online, in-person, or via phone; and leverage technology to break down barriers and increase communication between Federal agencies and the citizens they serve."[6]

"Agencies must be able to identify, credential, monitor, and manage user access to information and information systems across their enterprise in order to ensure secure and efficient operations. In particular, how agencies conduct identity proofing, establish digital identities, and adopt sound processes for authentication and access control will significantly impact the security of their digital services. Additionally, as information about individuals becomes more widely available through social media or through breaches of personally identifiable information (PII), it is increasingly important that all agencies adopt identity validation solutions that enhance privacy and mitigate negative impacts to delivery of digital services and maintenance of online trust. It is also essential that agencies' Identity, Credential, and Access Management (ICAM) strategies and solutions are informed by risk perspectives and driven by targeted outcomes."

2 https://policy.cio.gov/identity-draft/
3 https://policy.cio.gov/identity-draft/
4 https://www.fedscoop.com/icam-white-house-updates-policy/
5 https://www.fedscoop.com/icam-white-house-updates-policy/
6 https://www.performance.gov/CAP/CAP_goal_4.html

Unfortunately, to date most government agencies address ICAM with a combination of home grown, legacy offerings that are cobbled together over time. The result is limited capabilities, siloed data, fragmented security, expensive maintenance, and less-than-ideal user experiences. Yet, with the rise of security risks, online services, user demands, and the mandated initiatives listed above, identifying and implementing the leading digital identity platform capable of supporting ICAM for both internal and external use cases today and well into the future is an urgent priority for government agencies.

How to Use This Workbook

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

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

Use this workbook to compare digital identity management providers specifically for government and the public sector by copying the RFP question tables and filling in the blank answer boxes provided. ForgeRock answers are included within this workbook.

ICAM and CIAM Questions to Ask Digital Identity Management Providers for Government Agencies and the Public Sector

Provider:

RFP Question	Reason This Is Important To Ask	Provider Answer
Does the solution support identity and access management (IAM or IDAM) services for all external user use cases?	Traditionally, most agencies' focus has been on internal identities. However, due to digital transformation trends and increased demand, agencies need to offer citizens better access to on-line services. Strong identity and access management (IAM) capabilities and the security that comes with it is critical to achieving this mission to improve citizens on-line experience. Agencies that use IAM for external use cases realize improved citizen on-line experience and reduced costs.	
Does the solution have the capability of offering citizens the ability to authenticate with only the relevant information required to access on-line services?	Each governmental agency has unique requirements for authentication. For example, authenticating into the Internal Revenue Service (IRS) for personal tax information requires a different level of authentication than the Department of Interior (DOI) to reserve a camping site. A government-minded ICAM/CIAM solution should offer agencies the ability to customize the authentication criteria based on needs and requirements for every type of application.	

RFP Question	Reason This Is Important To Ask	Provider Answer
Does the solution allow users to grant granular access to their data with trusted third parties, such as other agencies or a user's relatives? Does the solution utilize privacy and consent standards such as the UMA 2.0 (user-managed access) standard?	Many citizens need to share access to their personal accounts with third parties such as family members, attorneys, and health care providers. To do this, the ICAM/CIAM solution must be able to support users granting and restricting account access, as well as selecting which account information can be shared with third parties, and which information should remain private. Future-minded ICAM/CIAM solutions utilize the UMA 2.0 standard to accomplish these capabilities.	
Can the solution secure APIs within a microservices architecture?	Microservices are an important development method that focuses on building and deploying applications as groups of modular, composable services within an application. Every aspect of the system is broken down to the smallest possible component. There are many advantages to a microservices approach, such as speed of development, resilience, speed of change, distribution of compute/bandwidth load, and reusability. Due to the many benefits, governments and agencies are utilizing and transitioning to microservices within their legacy environments. Within this reality, ICAM/CIAM solutions need to support microservices in order to track and secure access for people, things, and API's that share information internally as well as with third-party services.	
Does the solution support DevOps in order to respond quickly to existing and new regulatory and cybersecurity requirements? **Does the solution provide artifacts for deploying to the cloud using DevOps, Kubernetes, and Docker?**	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 management 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. Support for DevOps can dramatically decrease the time to roll out new services, features, and fixes necessary to respond to all citizen use cases. As a best DevOps practice, Docker is a tool used for containers and Kubernetes for the orchestration platform.	
Can the solution be deployed both on-premises and on any cloud environment, including multi-cloud, hybrid-cloud, and bring-your-own-cloud?	On-premises and cloud deployment options are essential to any best of breed solution. One size does not fit all and governments need options to support all of their legacy systems and environments, as well as those currently in the cloud and planned to be in the cloud.	
Can the solution support both new and legacy on-premises applications?	Citizen identity and access management should be implemented with an system-wide approach rather than stovepiped across several applications. Therefore the ICAM/CIAM solution needs to be flexible enough to support any application, from new to legacy.	
Does the solution enable federated citizen single sign-on (SSO) to all applications, including on-premises and external?	Citizens' demand frictionless authentication to access any and all agency applications with a single identity. To accomplish this, CIAM solutions should offer 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.	
Does the solution support secure citizen access from any device, including mobile?	Citizens are using devices such as mobile phones to access their accounts. ICAM/CIAM solutions should be able to support multi-channel access within a single system.	

RFP Question	Reason This Is Important To Ask	Provider Answer
Does the solution support the latest web authentication standards (FIDO2)?	It is critical to offer a variety of multi-factor authentication (MFA) solutions to secure the user. As detailed in NIST SP 800-63-3, FIDO2 is a web authentication standard that enables a strong authentication method for web and mobile. FIDO2 is a critical standard that allows government organizations to support strong MFA in addition to PIV (personal identity validation) and CAC (common access card) authentication. When used in combination with other factors, FIDO can achieve similar levels of authentication assurance as employee smart cards for citizen populations.	
Does the solution support a number of multi-factor authentication (MFA) options? **Does the solution easily support new form factors, including from a variety of third-party vendors?**	ICAM/CIAM solutions need to offer citizens choice because no citizen is the same and all have different user ability. Requirements change over time and an ICAM/CIAM solution needs to respond to the changes in the MFA market.	
Does your solution support open standards such as OpenID connect, Oauth, UMA 2.0 and others to support external use cases?	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 management providers are integrating standards that are needed to support 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. ICAM/CIAM providers committed to best-in-breed solutions will be active in standards bodies to ensure future capabilities. This helps organizations future-proof their investments.	
What privacy and consent capabilities does the solution offer to citizens? **Can users determine how their personal data is viewed and shared?**	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.	
How does the solution support integration with third party products that are necessary to meet expanded citizen use cases?	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 management 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.	

RFP Question	Reason This Is Important To Ask	Provider Answer
Can your solution help manage Identity of Things (IoT), such as stand alone IoT, non-person entities (NPE), and devices? **Can it address an IoT device's relationship to a personal identity?**	To create secure, personalized, omnichannel experiences, digital identity management 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.	
Can your solution provide Identity Proofing and does it offer integrations to a number of different options?	Identity Proofing is important to establish a high level of trust for both citizen and employee identities. A high-level assurance of identities enables government agencies to offer more online services and a better citizen experience to commercial organizations, such as CapitalOne or HSBC, or departments within other governments such as the United Kingdom National Health Services.	
How does the solution scale to support all external identities and roles across applications? **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?**	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 management 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 management 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.	
Can the solution be purchased from a managed service provider (MSP)?	Organizations have a variety of IAM use cases and many require different deployment options. Managed service providers offer customized deployment options compared to straight SaaS offerings. Further, they assist internal teams to deploy the solution to ensure accuracy and speed time to deploy/value. When selecting a solution, organizations should understand all the deployment options a vendor offers with MSPs, as customer needs may require different options over time.	
Does the solution offer the flexibility to be deployed either in modules or comprehensively?	Having the flexibility to deploy an ICAM/CIAM solution either in modules or as a comprehensive platform gives government entities the ability to extend and replace their current legacy investments at their own pace. ICAM/CIAM customers should partner with commercial providers that can compliment existing systems and then grow to a more comprehensive solution over time.	

This next section provides the ForgeRock answer for the same RFP questions listed in the tables above.

Provider: ForgeRock

RFP Question	Reason This Is Important To Ask	ForgeRock Answer
Does the solution support identity and access management (IAM or IDAM) services for all external user use cases?	Traditionally, most agencies' focus has been on internal identities. However, due to digital transformation trends and increased demand, agencies need to offer citizens better access to on-line services. Strong identity and access management (IAM) capabilities and the security that comes with it is critical to achieving this mission to improve citizens on-line experience. Agencies that use IAM for external use cases realize improved citizen on-line experience and reduced costs.	Yes. Identified as a customer identity and access management (CIAM) platform Overall Leader by KuppingerCole and the most visionary access management provider by Gartner, the ForgeRock Identity Platform is a flexible, unified solution consisting of access management, user-managed access, identity management, directory services, edge security, and an identity gateway. With standards, ease of integration, and operational fluidity at its core, the ForgeRock platform is able to support most user use cases, from simple authentication, to complex risk-evaluation, to personalized experiences.
Does the solution have the capability of offering citizens the ability to authenticate with only the relevant information required to access on-line services?	Each governmental agency has unique requirements for authentication. For example, authenticating into the Internal Revenue Service (IRS) for personal tax information requires a different level of authentication than the Department of Interior (DOI) to reserve a camping site. A government-minded ICAM/CIAM solution should offer agencies the ability to customize the authentication criteria based on needs and requirements for every type of application.	Yes. With the ForgeRock Identity Platform organizations can define their authentication options including multi-factor authentication (MFA), risk-based access control, and federated access management capability in a single solution across all areas required by the organization. Furthermore, the process of authentication can be adaptable to the context of the attempt to access protected content with dynamic evaluations and adjustments of the process itself to ensure high degrees of security and confidence.
Does the solution allow users to grant granular access to their data with trusted third parties, such as other agencies or a user's relatives? Does the solution utilize privacy and consent standards such as the UMA 2.0 (user-managed access) standard?	Many citizens need to share access to their personal accounts with third parties such as family members, attorneys, and health care providers. To do this, the ICAM/CIAM solution must be able to support users granting and restricting account access, as well as selecting which account information can be shared with third parties, and which information should remain private. Future-minded ICAM/CIAM solutions utilize the UMA 2.0 standard to accomplish these capabilities.	Yes. ForgeRock User-Managed Access 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.

RFP Question	Reason This Is Important To Ask	ForgeRock Answer
Can the solution secure APIs within a microservices architecture?	Microservices are an important development method that focuses on building and deploying applications as groups of modular, composable services within an application. Every aspect of the system is broken down to the smallest possible component. There are many advantages to a microservices approach, such as speed of development, resilience, speed of change, distribution of compute/ bandwidth load, and reusability. Due to the many benefits, governments and agencies are utilizing and transitioning to microservices within their legacy environments. Within this reality, ICAM/CIAM solutions need to support microservices in order to track and secure access for people, things, and API's that share information internally as well as with third-party services.	Yes. Creating value through your CIAM architecture means bridging the gaps between a 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. No other provider delivers the comprehensive capabilities to manage identity across an evolving microservices landscape. And, no other provider offers an end-to-end solution that checks all the boxes when migrating existing legacy applications to a microservices architecture.
Does the solution support DevOps in order to respond quickly to existing and new regulatory and cybersecurity requirements? **Does the solution provide artifacts for deploying to the cloud using DevOps, Kubernetes, and Docker?**	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 management 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. Support for DevOps can dramatically decrease the time to roll out new services, features, and fixes necessary to respond to all citizen use cases. As a best DevOps practice, Docker is a tool used for containers and Kubernetes for the orchestration platform.	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. 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).

RFP Question	Reason This Is Important To Ask	ForgeRock Answer
Can the solution be deployed both on-premises and on any cloud environment, including multi-cloud, hybrid-cloud, and bring-your-own-cloud?	On-premises and cloud deployment options are essential to any best of breed solution. One size does not fit all and governments need options to support all of their legacy systems and environments, as well as those currently in the cloud and planned to be in the cloud.	Yes. The ForgeRock Identity Platform deploys on premises as well as 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. The solution can also be architected for specific business or technical requirements with components being hosted in traditional data centers and the cloud simultaneously. Further, in addition to being the most advanced DevSecOp's platform designed to run in any Fedramp approved cloud (AWS, Google, Azure, OpenShift), Forgerock is launching an on-cloud offering in the Fall of 2019. Forgerock will also offer a full Platform-as-a-Service offering that allows customers to use every service in our existing on-premise solution.
Can the solution support both new and legacy on-premises applications?	Citizen identity and access management should be implemented with an system-wide approach rather than stovepiped across several applications. Therefore the ICAM/ CIAM solution needs to be flexible enough to support any application, from new to legacy.	Yes. ForgeRock fully supports both new and legacy applications. Modern applications are typically geared for use with identity propagation standards (such as federation) as well as integration points for authorization flows from a consistent interface. The ForgeRock Platform is not only able to accommodate uncommon use cases in such environments, but can also provide the framework for API-extensible requirements that would otherwise require costly customizations. There are many possible integration points between legacy solutions and the ForgeRock Identity Platform. The ForgeRock platform can be used to migrate legacy user repositories containing credentials and/or user profile data either immediately or over a defined period of time. It also offers several options for adding capabilities to legacy applications with limited or no built-in capabilities for user registration, authentication, authorization, or federation.
Does the solution enable federated citizen single sign-on (SSO) to all applications, including on-premises and external?	Citizens' demand frictionless authentication to access any and all agency applications with a single identity. To accomplish this, CIAM solutions should offer 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.	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 views open standards as vital to ensuring compatibility and interoperability with external systems, guarding against obsolescence, providing choice, and avoiding vendor lock in. Additionally, the Platform's flexibility often allows for supporting non-standards approaches to accommodate environments that, due to legacy or proprietary requirements, cannot be addressed with most other solutions.

RFP Question	Reason This Is Important To Ask	ForgeRock Answer
Does the solution support secure citizen access from any device, including mobile?	Citizens are using devices such as mobile phones to access their accounts. ICAM/CIAM solutions should be able to support multi-channel access within a single system.	Yes, ForgeRock provides many secure authentication modalities, both with embedded and external authenticators. These authentication options work equally well for mobile devices, and some options such as device fingerprinting and push notification, help use aspects of the device as factors. The strongest levels of authentication assurance as detailed in NIST SP 800-63-3 are implemented in ForgeRock authentication trees and can be used to achieve the highest levels of authentication even with mobile devices. The ForgeRock platform can also present access flows in a contextual manner, optimizing both the user experience and the security assurances desired.
Does the solution support the latest web authentication standards (FIDO2)?	It is critical to offer a variety of multi-factor authentication (MFA) solutions to secure the user. As detailed in NIST SP 800-63-3, FIDO2 is a web authentication standard that enables a strong authentication method for web and mobile. FIDO2 is a critical standard that allows government organizations to support strong MFA in addition to PIV (personal identity validation) and CAC (common access card) authentication. When used in combination with other factors, FIDO can achieve similar levels of authentication assurance as employee smart cards for citizen populations.	Yes. The ForgeRock Identity platform includes native support for the recently completed FIDO2 WebAuthn standard, meaning that users with FIDO2 WebAuthn compliant browsers (Chrome, Firefox, Microsoft Edge, etc) can take full advantage of either built-in or pluggable (USB) FIDO authenticators to log in and access resources and applications protected by the ForgeRock platform.
Does the solution support a number of multi-factor authentication (MFA) options? **Does the solution easily support new form factors, including from a variety of third-party vendors?**	ICAM/CIAM solutions need to offer citizens choice because no citizen is the same and all have different user ability. Requirements change over time and an ICAM/CIAM solution needs to respond to the changes in the MFA market.	Yes. MFA 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 (nodes are authentication purpose-built sub-components that modularly extend the Platform's capabilities). Additional node types are also provided on the ForgeRock Marketplace a single place to find best of breed MFA options that support changing security requirements.
Does your solution support open standards such as OpenID connect, Oauth, UMA 2.0 and others to support external use cases?	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 management providers are integrating standards that are needed to support 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. ICAM/CIAM providers committed to best-in-breed solutions will be active in standards bodies to ensure future capabilities. This helps organizations future-proof their investments.	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.

RFP Question	Reason This Is Important To Ask	ForgeRock Answer
What privacy and consent capabilities does the solution offer to citizens? **Can users determine how their personal data is viewed and shared?**	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.	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.
How does the solution support integration with third party products that are necessary to meet expanded citizen use cases?	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 management 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.	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.
Can your solution help manage Identity of Things (IoT), such as stand alone IoT, non-person entities (NPE), and devices? **Can it address an IoT device's relationship to a personal identity?**	To create secure, personalized, omnichannel experiences, digital identity management 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.	Yes. The core capabilities of the ForgeRock Identity Platform that 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. ForgeRock also recently released ForgeRock Edge Security, which offers complete end-to-end security for IoT deployments. The ForgeRock Identity Platform can also be used to model relationships between multiple different identities.

RFP Question	Reason This Is Important To Ask	ForgeRock Answer
Can your solution provide Identity Proofing and does it offer integrations to a number of different options?	Identity Proofing is important to establish a high level of trust for both citizen and employee identities. A high-level assurance of identities enables government agencies to offer more online services and a better citizen experience to commercial organizations, such as CapitalOne or HSBC, or departments within other governments such as the United Kingdom National Health Services.	Yes. Identity proofing can be achieved by adding desirable processes in the user self-service configuration. Verification steps can also be added to an authentication tree, typically leveraging a scripted decision node. These registration and verification nodes can leverage either internal validation data structures (such as a user database that contains application-specific data) or external services that provide targeted analysis of a user's claimed identity in conjunction with government-sourced data (such as the DMV). Additionally, partners from the ForgeRock Trust Network, such as Daon and Callsign, are among the strong authentication vendors that have developed authenticators for use with the ForgeRock Identity Platform and can be utilized for identity-proofing purposes.
How does the solution scale to support all external identities and roles across applications? **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?**	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 management 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 management 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.	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.
Can the solution be purchased from a managed service provider (MSP)?	Organizations have a variety of IAM use cases and many require different deployment options. Managed service providers offer customized deployment options compared to straight SaaS offerings. Further, they assist internal teams to deploy the solution to ensure accuracy and speed time to deploy/value. When selecting a solution, organizations should understand all the deployment options a vendor offers with MSPs, as customer needs may require different options over time.	Yes. Forgerock has a network of Approved Deployment Partners who can help organizations deploy the ForgeRock Identity Platform on-premise or provide managed solutions. For example, Deloitte currently offers Forgerock as part of their digital services offering. This offering is running as FedRamp Medium approved.
Does the solution offer the flexibility to be deployed either in modules or comprehensively?	Organizations have a variety of IAM use cases and many require different deployment options. Managed service providers offer customized deployment options compared to straight SaaS offerings. Further, they assist internal teams to deploy the solution to ensure accuracy and speed time to deploy/value. When selecting a solution, organizations should understand all the deployment options a vendor offers with MSPs, as customer needs may require different options over time.	Yes. Forgerock has a network of Approved Deployment Partners who can help organizations deploy the ForgeRock Identity Platform on-premise or provide managed solutions. For example, Deloitte currently offers Forgerock as part of their digital services offering. This offering is running as FedRamp Medium approved.

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

ForgeRock: Defining Digital Identity Management

ForgeRock: Defining Digital Identity Management Identified as a 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 leads and shapes 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 — citizens, employees, customers, devices, and 'things'. The ForgeRock Identity Platform consists of access management, user-managed access, identity management, directory services, edge security, and an identity gateway. The full platform can 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*.

ForgeRock has a wealth of experience supporting IAM solutions across all industries and global governments. In the US market, ForgeRock supports and enables ICAM solutions at the United States Internal Revenue Service (IRS), Department of Homeland Security (DHS), General Services Administration (GSA), National Oceanic and Atmospheric Association (NOAA), and the US Navy. Additionally, ForgeRock supports non-governmental organizations (NGOs) such as the National Science Foundation (NSF) and their Educational Grant Program. Further, ForgeRock is active within global governments such as Norway, Canada, the United Kingdom, Australia, Germany, Belgium, New Zealand, and others. ForgeRock also has active IAM programs across state, provincial, and local governments within the US and Canada. Examples include the State of Utah, State of Texas, the Province of Alberta, and the city of Richmond British Columbia.

Learn More About ForgeRock for Your Organization

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