ForgeRock®

White Paper

10 IAM Capabilities Key for Governments to Support Citizen Access

How to Give Citizens Secure, Seamless Access to Government Services from Anywhere

The demand for online government services has skyrocketed. Governments must now provide secure web and mobile access to services for millions, and even billions, of citizens while complying with regulations such as GDPR. Additionally, they must also support various levels of security credentials that are different from one country to another. Yet, traditional IT environments and legacy identity and access management (IAM) systems are being pushed to their limit by this. They weren't built to support such a massive volume of citizens from widespread locations. The result is a latency, frustration, friction, increased risk, and poor user experience — resulting in government leaders like you to ask how to quickly and easily support online citizen access at scale without upending operations or compromising security and user experience.

The following are 10 modern IAM capabilities that can be easily incorporated into your IAM infrastructure to support remote citizen access at today's massive scale.

10 IAM Capabilities Key for Governments to Support Online Citizen Access at Scale

1 Availability and Scale

To keep your government services going and make citizen experiences fantastic, it is important to ensure that a user's access and session remains undisrupted should something happen, such as a server going down. Modern IAM platforms should include both service availability and session availability. Service availability ensures that users can access a site when a server goes down. Session availability preserves and keeps a session running if a server goes down.

Modern IAM should also support a variety of scale scenarios. This includes an ever-changing number (often millions) of users, devices, and things, as well as changing frequencies and lengths of simultaneous and concurrent sessions. Additionally, to help maintain healthy services and protect against breaches and distributed-denial-of-service (DDoS) attacks, you should leverage an Identity Gateway to monitor API traffic, throttle traffic volume, and detect anomalies.

Modern IAM platforms should include service availability, session availability, and support a variety of scale scenarios

2 Custom Authentication Journeys

As citizens, we all want fast, frictionless access to government services. At the same time, governments need to protect us, our data, and their assets from fraud and cyberthreats. By customizing authentication journeys with factors such as user type, device, and geolocation, as well as using self-service features such as self-registration or password reset, you can reduce friction during the authentication process in order to provide a great user experience. On the flip side, you can also add friction, such as multi-factor authentication, when there's suspicious activity.

Support for Zero Trust/CARTA Security Models

3

It's a sad reality that fraud and cybercrime have persisted and even risen in the wake of current events. Zero Trust/Continuous Adaptive Risk and Trust Assessment (CARTA) security models are based on the idea that no network, individual, thing, or device can be trusted. Modern 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 these models, every action taken must be properly authenticated and continuously authorized. To do this, authentication and authorization decisions take into consideration a rich set of information by leveraging contextual information and become risk-based rather than binary.

> In the wake of the COVID-19 pandemic, fraud and cybercrime have persisted and even risen

Privacy, Consent, and Regulatory Support

4

To support remote citizen access requires that you comply with the various regional regulations (such as the California Consumer Privacy Act [CCPA] and the General Data Protection Regulation [GDPR]) that apply to your citizen locations. For compliance, it's critical that modern IAM platforms enable you to meet regulation and compliance standards. This includes Privacy by Design and Consent mechanisms based on the UMA 2.0 standard, as well as integration with other software that helps meet regulatory requirements.

Equally important, to provide a great experience for your citizens, you also need to make it easy for them to register, consume, and manage their personal preferences or run the risk that they will leave for a better experience offered by competitors. Modern IAM platforms should include intuitive and user-friendly privacy and control mechanisms that make it easy to register and manage profile and privacy settings.

API Security

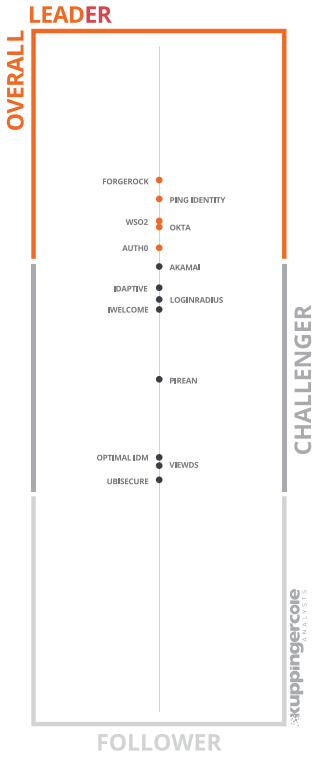
5

APIs make today's remote world go round by linking people, systems, and services together, no matter where they are. As detailed by KuppingerCole in their API Security Leadership Compass report and Modern Identity Fabrics research paper, API security is a linchpin of modern identity and access management strategy.

With identity-enabled APIs, you can:

- Meet citizen expectations by delivering seamless, omnichannel experiences
- Create value-added citizen services through partnerships and third-party integrations
- Bridge legacy systems with modern applications
- Aggregate citizen data from multiple systems into a single view

To secure APIs requires a standards-based, modern IAM platform capable of exposing rich APIs for seamless integration, deployment agility, and continuous delivery. Modern IAM platforms also leverage a gateway to secure APIs and users by enforcing authorization for any type of traffic. You can also monitor API traffic, throttle traffic volume, and detect anomalies.



KuppingerCole names ForgeRock "Overall Leader" in all categories for API Security

Progressive Profiling

6

To enhance the citizen experience, rather than asking citizens to fill out extensive registration forms, you can implement progressive profiling, a technique to collect citizen information as they interact with your system, on your website or application. For example, you might collect just the citizen's name, citizen identification number, and password on initial signup. At a later point in time, you might ask for their email address and physical address.

A Unified Experience Through a Single View of the User

7

Poor citizen experiences create frustration and result in needing additional government resources to resolve issues. From an IAM perspective, a disjointed view of a user is often the source of poor experiences. Citizens use services across many different government agencies. There may be citizen data integration between some agencies, but on the whole, data about a citizen is typically siloed. This presents difficulties in fully understanding and providing citizen services from a 360-degree view. This includes knowing all their access rights, preferences, usage, potential risks, and more. Unfortunately, legacy IAM cannot bridge the siloes to help solve the puzzle.

In order to gain a complete picture of your users and how they interact with your organization, modern identity and access management (IAM) uses identity management and directory services products to synchronize, migrate, and manage identity data across your government or agency's system environment.

With a single view of a user, you're then able to:

- Give citizens the option to use the same single identity when they access various public portals
- Consolidate user identities and increase their security with behavioral, contextual, and risk-based authentication and authorization policies
- Standardize and unify the citizen experience across any device (omnichannel)
- Continuously gather information about citizens in a streamlined, non-intrusive way (progressive profiling)
- Increase online citizen acquisition and retention with easy registration and exceptional, personalized experiences
- Conduct analytics on profiled user bases to better understand citizens and risks

The State of Utah integrated and unified over 900 applications, resulting in over $15 million in savings. Read the case study

Easy Technology Integrations

8

To address today's requirements and be prepared for tomorrow's, the strongest digital identity solutions are those that integrate easily with a wide variety of other technologies, such as strong authentication, risk and fraud management, behavioral biometrics, and identity proofing and enrichment. As such, government leaders should seek solutions from digital identity providers that have a strong ecosystem of respected consultancy, technology, and integrations partners. This partner ecosystem should be designed to immediately support your needs with easy integration, as well as be a source of collaboration and innovation for the future.

DevOps Friendly Architecture

9

Time is of the essence when it comes to developing and deploying capabilities that support online citizen access to government services. One of the best ways to improve speed to market is to adopt a DevOps model.

DevOps enables software development and deployment cycles to run continuously, so you can roll out new apps, services, and capabilities faster by reducing time to production. Because of the efficacy and rapid adoption of DevOps, future-minded IAM platforms support DevOps deployment with containerization and orchestration technologies such as Docker and Kubernetes.

DevOps-friendly IAM platforms help you roll out new apps, services, and capabilities faster

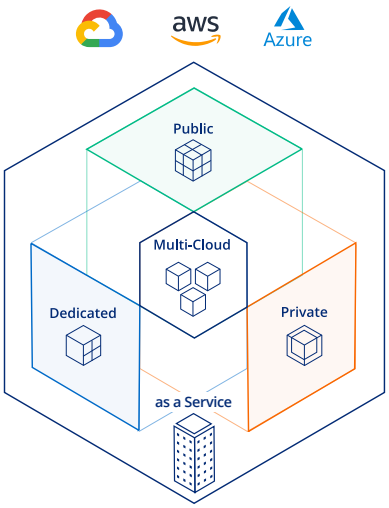
Flexible Cloud Options to Consume or Deploy

10

Today, implementing modern IAM capabilities that securely support online citizen access to government services quickly is important. Traditional, legacy IAM deployment and maintenance is often lengthy, costly, and complex, requiring numerous resource hours and slowing time-to-market. Further, legacy IAM solutions can be very difficult to modify in order to meet new needs, trends, and demands. On the flip side, consuming or deploying modern IAM in the cloud accelerates time-to-market, increases flexibility, availability, and scalability, and saves resource time.

By deploying a modern IAM platform in a cloud environment (such as private, public, hybrid cloud, multi-cloud) or consuming it as a service (IDaaS), you can easily move your existing workloads and and get up and running within minutes without sacrificing rich features and extensibility. Further, with an identity platform as a service, you also get the benefit of offloading maintenance to the provider, as well as the big advantage of always being on the latest version.

Importantly, IAM providers that offer their platform as a service with feature parity to their software offering gives you the invaluable flexibility to easily shift your IAM environments according to your needs with minimal disruption.



The ForgeRock Identity Platform: Deploy in the Cloud or Consume as a Service

Connect Everyone, Anywhere With ForgeRock

Identified as a leader in Consumer Identity and Access Management (CIAM) by Forrester® and KuppingerCole, a leader in Access Management by Gartner®, and the Overall Leader in all categories for Identity API Platforms by KuppingerCole, the ForgeRock Identity Platform helps governments and agencies provide online citizen access at scale without sacrificing experience and security.

> "Overall, ForgeRock is amongst the leading-edge vendors in the IAM space and should be considered in product evaluations."
>
> – KuppingerCole

ForgeRock helps people safely and simply access the connected world by enabling exceptional digital experiences, no-compromise security, and comprehensive functionality at any scale. The ForgeRock Identity Platform consists of Identity Management, Identity Governance and Administration, Autonomous Identity, Access Management, User-Managed Access, Directory Services, Edge Security, and an Identity Gateway. The platform is delivered as-a-service and with push-button deployments to any cloud or any data center.

Meet Modern Identity Requirements Without Ripping and Replacing Legacy IAM

Today, time is of the essence. Unlike most IAM providers, with ForgeRock you don't need to suffer the pain, risk, and expense of ripping out existing legacy identity solutions to get the features and benefits of IAM modernization needed to support your healthcare business at scale.

ForgeRock provides a flexible approach that enables you to augment first, then coexist to later consolidate or retire disparate, legacy identity management systems like CA Single Sign-On (SiteMinder), Oracle, IBM and even homegrown identity systems.

ForgeRock provides a flexible approach that enables you to augment first, then coexist to later consolidate or retire disparate, legacy identity management systems

We're Here and Ready To Help. Contact Us to Get Started

Government leaders use ForgeRock to facilitate their online citizen services, increase productivity, mitigate risk, and reduce costs. Contact us to learn more about how ForgeRock can help you.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com or follow ForgeRock on social media.

Follow Us

ForgeRock