FORGEROCK /White Paper

/Improving the Quality of Government Services with Citizen-Focused Identity Management

Improving the Quality of Government Services with Citizen-Focused Identity Management

Today, many government agencies store and manage the data for all their disparate online services in separate silos - and the silos cannot communicate with one another. Users have to sign in to each service separately, using a different user name and password. Agencies wishing to improve the user experience by integrating their back-end systems via a single web portal find that it is a costly and complicated process.

The key to solving this problem lies in harnessing the power of a strong user identity for the benefit of both government agencies and the citizens and businesses they serve. With a strong identity management platform, government agencies can tie all their disparate services together into one, cohesive service accessed through a single portal. Users need access the portal just once, via a single sign-on, to access all services, such as renewing a license, paying a fine, filing taxes, or renew a passport. Everyone - government agencies and users alike - benefits from enhanced service interactions, accelerated service deployment, and fewer fraudulent transactions.

Employing citizen-focused identity and eliminating the traditional silo approach to delivery allow government agencies to be more proactive in providing services and streamlining delivery. In addition, citizens and businesses will see the immediate benefits and value of government agencies monitoring and managing their online behavior on disparate devices such as laptops, mobile phones, tablets, wearable technology, or other connected innovations. At the same time, this approach future-proofs government agencies' identity management models. This guide is designed to help agencies understand how an identity management strategy makes it possible to provide simple, secure access to a wide range of digital public services.

What is Citizen-Focused Identity Management?

Because federal, state, and public organizations are beholden to numerous regulatory compliance and privacy policies, they must leverage citizens' identity to safely and securely offer them access to a multitude of public and federal services across any channel. Government organizations are just starting to realize the benefits of the cloud, mobility, and the Internet of Things (IoT). They are finding new opportunities to conduct routine public activities online and thus improve services ranging from tax procurement to acquiring birth and death records, applying for government-backed student loans, and more.

Government organizations also recognize the enormity of managing the digital identities of every citizen while simultaneously securing information and adhering to strict compliance policies as they transition sensitive, classified information to completely digitized systems. Legacy identity access management (IAM) technologies leveraged monolithic platforms that used static rules to make decisions. Such technologies were not designed to easily integrate with any application (on premises or off), to provide device-agnostic access, handle large-scale populations, or make decisions based on government policy and user context. In short, traditional IAM cannot meet the need for accuracy, efficiency, security, and privacy. To connect citizens to necessary public services in the digital age, governments will now require citizen-focused identity management.

Citizen-Focused Identity Management Delivers Many Advantages

- It implements a common, secure identity platform throughout the government agency for sharing valuable data across different departments while also protecting user privacy.
- Provides a common platform across departments that makes service deliveries easier and reduces total costs. For example, each citizen has only one identity, and the agency has only one support center.
- Brings services to citizens: citizens are not brought to services. Access from anywhere, from any device provides real-world value by enabling citizens and businesses, as this is how they expect to consume services today and into the future.
- Delivers services more quickly and efficiently.
- Uses real-time context to make access and security decisions and to offer personalized services based on citizen needs and profiles.
- Provides a single user overview across the organization.
- Takes advantage of a modular, scalable, and flexible architecture to facilitate repeatable processes, accommodate millions of concurrent users and devices, and enable deployment times faster than those of typical legacy systems.

Citizen-focused identity management uses identity to break down agency silos and create a single, agency-wide view of the citizen while also protecting user privacy. It uses data to build citizen profiles that help government agencies engage with citizens effectively. Because this new identity management is specifically designed for citizens—built for flexibility, scale, and the IoT—it interacts with e-citizen portals and yet-to-be-invented technologies on which governments will rely in the years ahead. Understanding who these citizens are and what they need enables governments to provide more relevant and efficient services that vastly improve the user experience, which in turn allows further expansion of necessary services and initiatives that capitalize on this new user data.

Key Takeaway: Traditional IAM cannot meet the need for accuracy, efficiency, security, and privacy. To connect citizens to necessary public services in the digital age, governments will now require citizen-focused identity management.

Unified Identity Model Accelerates the Delivery of Public Services

Today, identity management platforms must cater to the specific needs and demands of the citizens who use them. Unfortunately, agencies that have relied on traditional IAM and/or home-grown systems, typically cobbled together from disparate technologies, have been saddled with unwieldy, overly complex “product suites” replete with redundancies and compatibility issues. These product suites are notorious for taking years to deploy and integrate, which leads to failed or seriously delayed projects. Niche IAM vendors created streamlined solutions to address specific problems, but without any overarching identity solution, agencies had no way to quickly and easily build, secure, and manage consistent citizen identities across departments.

To make it easy to roll out new services or enhance existing ones, government service providers need a unified identity model underpinned by the principle that identity should be exposed in a single, repeatable way. This principle is driven by the primary goal of providing new public services quickly, reducing implementation time from years to merely weeks.

Key Takeaway: It is essential that agencies have a common identity platform with a single, repeatable API that enables developers to implement identity services. This implementation process must be repeatable, easy for developers to use, and ensure reliability, flexibility, trainability, and agility.

Identity Management Provides Stronger Security and Compliance, Reduces Fraudulent Requests

In addition to making public services more efficient, today's identity management solutions help bolster online security and resolve compliance woes, making them an integral part of any robust, multi-layered security model. In addition to credentials, real-time contextual clues help government agencies vet the user's level of access.

For example, when a system detects a login attempt with correct credentials, but from an unrecognized IP address or at an atypical time of day, the software triggers additional security precautions. These include asking security questions or texting verification codes to a user's cell phone.

Key Takeaway: Your identity management platform must support dynamic decision-making based on real-time context. Static approaches to evaluating access and authorization policies limit your ability to properly protect your most important asset—the citizen.

Practical Application: Reducing Government Costs While Delivering Services to a Connected Population

To ensure the security of information, Norway's Agency for Public Management and eGovernment implemented a central authentication and single sign-on service for the different government agencies in Norway. This solution enables citizens to use the same login portal regardless of which public services they intend to access. This central service is called ID-Porten and has been implemented as a hub and spoke architecture. The Government of Norway uses at the center of the ID-Porten the ForgeRock OpenAM.[1]

The hub, ID-Porten, is at the center of the architecture. Government agencies such as the tax office, labor and welfare agency, health economics administration agency and water and energy directorate, are the spokes that use the authentication and single sign-on services of ID-Porten. The ID-Porten implements several levels of authentication: MyID whish uses PIN code authentication, BankID—a bank-issued electronic ID, Buypass, a private electronic ID that can also be used to bet online in Norway, and Certificates which are stored in USB pens and issued by a private company called Commfides.

The federation technology used as the hub and spoke architecture is SAML 2.0. The ID-Porten uses OpenAM to implement a SAML 2.0 Identity Provider with multiple authentication contexts that are mapped and plugged-in within the OpenAM federation and authentication framework. In this way, each of the authentication eIDs can be associated with different authentication contexts and different authentication strengths. The flexibility of the OpenAM architecture enables the team to extend and modify the architecture to quickly support additional eIDs when required.

Thanks to the SAML 2.0 federation standard, the governmental agencies can use any SAML 2.0 Service Provider implantation to use the ID-Porten services.

With ForgeRock, Norway's eGovernment portal delivers:

- Secure, single sign-on for 5 million citizens and 500,000 businesses
- Reduction in identity theft and increased trust in online identity
- Estimated annual government cost savings of USD $68 million

[1]Government of Norway Case Study: https://www.forgerock.com/app/uploads/2015/06/case_study_norway_letter.pdf

Taking a Customer Approach to Citizen Engagement

Successful organizations typically take a customer-first approach to the customer engagement experience. Government agencies could certainly learn from these organizations' best practices. Some of these best practices are easy to implement and do not compromise agencies' ability to comply with security or compliance regulations.

The following list highlights a number of best practices employed by the private sector.

- **Single sign-on** – This gives citizens easy access to all of the dedicated services they are eligible for.
- **High scalability** – As populations and services rarely decrease, it is critical that the back-end infrastructure be able to scale as the population grows and new services are added.
- **Flexibility** – Deployment of new, scalable services to the cloud and mobile devices is managed through one access management platform
- **Fraud prevention** – Best practice employs a two-layer strategy. Contextual information evaluates the risk of citizens attempting to access resources, and if an identity is deemed suspicious, a higher level of authentication or identity-proofing ensures the citizen is real.
- **Delivery** – Services need to be built so they can be accessed by – and in some cases consumed – from any device, anywhere, and at any time of day. They must also be ready for the technology of the future.
- **Security** – Government agencies need to deliver services to citizens and businesses transparently while still maintaining a secure channel for transactions. The core infrastructure must be secured to ensure protect the identity of citizens and business as well as the services they use.

Key Takeaway: Citizens and businesses interact with - and consume services at - all levels of government. They have come to expect the ability to make transactions anywhere, on any device, at any time of day, similar to mainstream consumer services. There is no reason why governments cannot anticipate and act on the services that citizens and business are coming to expect.

Does Your Current Identity Management Solution Support Privacy?

Every citizen's deepest fear is that his or her data will be compromised. Fortunately, citizen-focused identity management was designed from the ground up for large-scale, citizen-facing deployments. Such a system is not merely legacy IAM pushed to its limits trying to accommodate an ever-changing digital landscape. Rather, the system is designed to connect to many users and devices at once, and to react quickly to context, shutting down access from an unfamiliar device or blocking entry to data that is not applicable to the user.

Citizen-focused identity management also supports standards like OAuth2, OpenID Connect, System for Cross-domain Identify Management (SCIM), and perhaps most importantly, User-Managed Access (UMA). UMA lets a citizen control the authorization of online apps and services to share his or her data.

Key Takeaway: Identity is a citizen's last line of defense when it comes to security. If a credential is stolen, real-time context must be used to evaluate risk and protect against unauthorized access. A citizen-focused identity management solution is able to manage risk and use real-time contextual data to handle access requests and policy enforcement.

Can Your Current Identity Management Support Large-Scale Populations?

Because they are designed for the Internet, citizen-centric identity management solutions are built for high traffic and high volume and can support millions of concurrent users.

Key Takeaway: Legacy platforms were designed for employees located on business premises and cannot stand up to current and future digital-government demands. Citizen-focused identity platforms are designed to accommodate Internet scale and support a variety of devices, with citizen ease of use in mind.

What's the Best Way to Evaluate an Identity Management Solution?

To evaluate an identity management solution effectively, agencies should make sure it meets the requirements listed below. Potential vendors should clearly outline how the solution will work to meet each of an agency's requirements. Finally, agencies should test the solution. A thorough evaluation up front will save years of toil and trouble down the road.

It is important to be aware that some vendors will pitch a pre-fab demo. Ask to see a real, live proof of concept (POC). Any vendor can claim to have a modular, lightweight, flexible stack, but the proof is in the pudding; if it takes 20 engineers 20 days to simply install the software, the system is not what it claims to be. If you do not understand how the solution will work for your agency, proceed with caution until you do.

Key Takeaway: To help you in your buying process, make sure the following boxes are check-marked before you commit to a citizen-facing identity solution. Some companies offering citizen-facing identity suites have not built a new platform but are instead repurposing a legacy IAM solution. If the solution meets the requirements below, it is a genuine identity management stack, ready and able to solve your citizen-facing identity needs.

- ☐ **1.** Was it designed for citizens and large populations, or for employees?
- ☐ **2.** Is it context-aware?
- ☐ **3.** Can it enable citizen-facing services?
- ☐ **4.** Can it produce a uniform citizen profile across departments?
- ☐ **5.** Is time to market weeks to months, or months to years?
- ☐ **6.** Is it device-agnostic?
- ☐ **7.** Is it highly scalable?
- ☐ **8.** Are processes repeatable, so you can roll out new services without starting from scratch each time?

Additional Resources

Learn more about how the Government of Norway implemented citizen-focused identity management:

For more information on the ForgeRock Identity Platform

About ForgeRock

The ForgeRock Identity Platform™ transforms the way millions of customers and citizens interact with businesses and governments online, providing better security, building relationships, and enabling new cloud, mobile, and IoT offerings from any device or connected thing. ForgeRock serves hundreds of brands like Morningstar, Vodafone, GEICO, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, among many others. Headquartered in San Francisco, California, ForgeRock has offices in London, Bristol, Grenoble, Oslo, Singapore, and Vancouver, Washington. ForgeRock is privately held, backed by leading global venture capital firms Accel Partners, Foundation Capital, and Meritech Capital. For more information and free downloads, visit https://www.forgerock.com or follow ForgeRock on Twitter at http://www.twitter.com/forgerock.