Identity Platform: Forging a New Future with Identity Relationship Management

A Reference Architecture for Customer Identity and Access Management (CIAM)

Table of Contents

Executive Summary

Identity and access management (IAM) was originally designed for a company's internal use, to deal with manual on and off-boarding, and to set up access privileges for company data and systems behind the firewall. Today though, companies need to implement dynamic IAM solutions that support not just employees, but customers and their many digital devices. IAM needs to handle employees as well as partners, prospects, customers, and devices, regardless of location.

ForgeRock® is ahead of this curve, first introducing the new IAM industry standard, Identity Relationship Management, in 2013. We were built from the ground up with the shift from internal, on-premises IAM to identity relationship management (IRM) in mind. Our IRM platform is customer-facing, secure, scalable, and accessible. It makes digital identity management a business asset, rather than a security cost center.

ForgeRock's next-generation IRM platform is designed to give CEOs and enterprises the power to engage with their partners, prospects, and customers through new revenue-generating digital services, while continuing to provide proven, traditional IAM capabilities as icing on the cake.

Introduction

Business, education, and government institutions use identity management platforms to regulate the identities of individuals and devices, and their associated attributes, credentials, and entitlements organization-wide. Today, identity relationship management is necessary both on and off-premises, increasingly important for managing users and their devices in mobile, social, and cloud environments. Legacy identity management solutions were not built for cloud compatibility, device-agnostic access, high volume, or customer engagement, and most were built by acquisition, rather than designed to work as a cohesive whole. This makes them inherently:

- Inflexible
- Difficult to Implement
- Complex to Integrate
- Convoluted
- Limited in Scale
- Locked In
- Expensive
- Inaccessible to Developers

Solutions must be flexible enough to support new customer-facing mobile, social, web, and cloud app projects, while providing seamless integration with legacy systems. Platforms should be purpose-built to work together anywhere, so clients are never saddled with the costs of acquisitions. Agile organizations need solutions that are:

- Adaptable
- Simple to implement
- Modular
- Lightweight
- Highly scalable
- Plausible to exit
- Developer-friendly
- Cost-effective
- Flexible

Identifying and targeting these solution benefits is especially critical now, during this transition period from traditional, on-premises IAM to mobile, social, web, and cloud-compatible IRM platforms, as businesses make decisions about their future identity strategies. Making a great identity decision will not merely protect company and customer data; it will allow the organization to shift away from the burden of supporting legacy systems, to investment in solutions that accelerate innovation and drive top-line growth.

Business Pain Points

Traditional, employee-facing IAM struggles to meet the evolving requirements of customer identity management in the following ways:

Inflexible

Traditional, employee-facing IAM is designed for specific static events, but in today's IRM world, systems must understand and react to contextual circumstances to determine whether or not you get access, and if so, how much and to what. If you log in from a new device or from a different country, for example, a modern, adaptable IRM system will adjust to the uncertain circumstances and ask you for additional authentication beyond a simple password.

Difficult to Implement

Many traditional IAM solutions were built by acquisition, chock full of varying APIs, documentation, libraries, and protocols with no consistent standard of operation. Developers waste valuable time learning how all the parts and pieces work, instead of modifying, customizing, and streamlining the platform to suit unique business needs.

Complex to Integrate

It's common for IAM suites to demand a rip and replace migration process from clients' existing platforms. Developers looking to incorporate new solutions into existing IAM strategies find their legacy suites are not designed for customization or to work well with other systems.

Traditional IAM—typically built piecemeal through acquisitions, tacking on parts as needs arise—struggles to respond to the multitude of users, circumstances, devices, access points, and access privileges that dominate today's IRM world.

Convoluted

Designed for the old world of on-premises IAM security, these solutions generally rely on heavyweight APIs and complex standards that are only accessible to developers and architects with specialized identity knowledge.

Limited in Scale

Traditional IAM platforms were designed to protect the security perimeter and employees only, making them difficult to adapt for the modern enterprise, which must maintain mobile, web, social, cloud, and on-premises identity data simultaneously in order to satisfy client, customer, and employee IRM needs. As the number of users grows exponentially, modern IRM systems must be able to accommodate hundreds of millions of additional identities instantaneously, achieving a scalable volume that was neither possible nor needed for the enterprise, but is essential in an internet-connected, customer-facing world.

Locked In

Proprietary solutions are infamous for rip and replace migration strategies and vendor lock-in contracts. Once an enterprise has experienced the lengthy, painful process of moving all IAM data and operations to the new platform, they are unlikely to want to repeat the process again soon, whether or not they are satisfied with the platform. And when the contracts come up for renewal, high-pressure legal tactics are used to force enterprise customers to immediately renew in order to avoid using the product in breach of contract.

Expensive

Contracts with legacy vendors famously begin with a discount, but then quickly ramp up in maintenance and subscription fees, gouging customers for every feature and up-sell. High-pressure tactics are used to elicit renewals at a significantly higher price point, and clients are hesitant to go through another round of painful rip and replace migration. The costs are always high because the customer pays for the acquisitions that built their IAM platform.

Inaccessible to Developers

Legacy IAM platforms built by acquisition are saddled with a whole host of disparate APIs, libraries, documentation, etc., hindering the developer's ability to learn, make adjustments, tailor solutions, and teach others to use the platform, giving developers limited maneuverability to innovate.

Business Trends

Enterprises require a new, modern solution that can meet the rapidly growing need for highly effective IRM, internally and externally. The number of people, services, and things to manage is growing exponentially, and increasing numbers of applications are moving to the cloud and other devices as the internet of things grows. Businesses need to engage with customers and offer better and more personalized user experiences that drive loyalty and spending, giving them an edge over the competition as they take on the hefty task of digital transformation—and they must do so with their customers' privacy in mind.

Today, effective security demands integrated, contextual, and highly scalable identity data, efficient, trusted, customer-facing services, and developer-friendly ways to support the growing milieu of users, devices, (laptops, phones, touch pads, cars, cameras, etc.), and mobile, social, web, and cloud applications (on or off premises). CIOs must invest in IRM solutions because identity management is now a business driver that connects customers, partners, employees, and users, directly impacting top-line revenue, customer relationships, and business reputation. This is the evolution of IAM to IRM: Identity Relationship Management.

This shift in business emphasis has a direct technical impact on how we think about identity and access management. Managing risk, privacy and consent, auditing, reporting, and compliance are ongoing costs of business that an effective identity management strategy should continue to address. The right identity relationship management solution will also actively contribute to essential top-line growth by adhering to the pillars of IRM outlined on the following page.

Customers and Things Over Employees

Traditional IAM platforms were designed for on-premises employee use and are unable to provide the quick, secure, and device-flexible IAM experience customers are looking for. Modern identity management must manage access privileges for all stakeholders across a variety of devices.

Customer Trust and Privacy Over Risk Management

Legacy IAM was not designed to manage personal data privacy expectations between individuals and

organizations in the digital era. Privacy and compliance regulations similarly lag behind, are imprecise and insufficient. Today's IAM solution must take a proactive and standards-based approach to address privacy regulations like the General Data Protection Regulation (GDPR), establish and protect customer data, privacy, and trust in new digital offerings. Organizations should empower users to conveniently update their sharing preferences across an entire digital ecosystem. And users should be able to share specific personal data—and withdraw it at will. Personal data autonomy is the bedrock of data privacy.

Adaptable Over Predictable

Unlike traditional IAM designed for specific static events, IRM must understand contextual circumstances. For example, a legitimate user logging in from a different device or location should be granted access to the information they need, while others are shut out.

Top-line Revenue Over Operating Expense

IAM was always considered a necessity for employees and therefore a business cost. In today's world, the security system is used to authenticate and authorize both customers and employees. If an IRM solution is efficient, secure, trusted, and accurate, it can directly contribute to a business' top-line revenue, as customers will have easy access to secure applications where they can buy services.

Velocity Over Process

IAM has migrated from business cost to business driver. Companies suffer materially if their IAM solution takes too long to deploy, adapt, or respond to user events. Employees had to put up with slow IAM systems, but customers don't and won't. Modern IRM serving employees, customers, and devices must instantly react to variable circumstances and events, and must be massively scalable and available so that no user ever waits around–or worse, is shut out. CIOs today make IRM decisions based on time to deploy, ease of use, and the ability to scale to handle customer volume—not just on license and deployment costs.

This shift in business emphasis has a direct technical impact on how we think about identity and access management. Through this shift we have come to value.

Internet Scale Over Enterprise Scale

Today's users access secure systems not just on premises, but in the cloud and via the internet, any time, day or night. Today's users are not just employees logging on at work but also partners, customers, and devices signing in from anywhere. As the number of users grows exponentially, modern IRM systems must be able to accommodate hundreds of millions of additional identities instantaneously, achieving a scalable volume that was neither possible nor needed for the enterprise, but is essential in an internet- connected, customer-facing world.

/PILARS OF IRM

Business Pillars

- **Customers and things** over employees
- **Customer trust and privacy** over risk management
- **Adaptable** over predictable
- **Top-line revenue** over operating expense
- **Velocity** over process

Technical Pillars

- **Internet scale** over enterprise scale
- **Dynamic intelligence** over static intelligence
- **Borderless** over perimeter
- **Modular** over monolithic
- Deploy on-premise or in the cloud, including AWS, Azure and others.

Dynamic Intelligence Over Static Intelligence

Traditional IAM was designed for a specific set of events – employee on and off- boarding, for example, taking place in a predictable on-premises work environment. Today's IRM must understand the circumstances in order to determine whether or not you get access, and if so, how much and to what? If you log in from a new device or from a different country, for example, a modern, adaptable IRM system will adjust to the uncertain circumstances and ask you for additional authentication beyond a simple password.

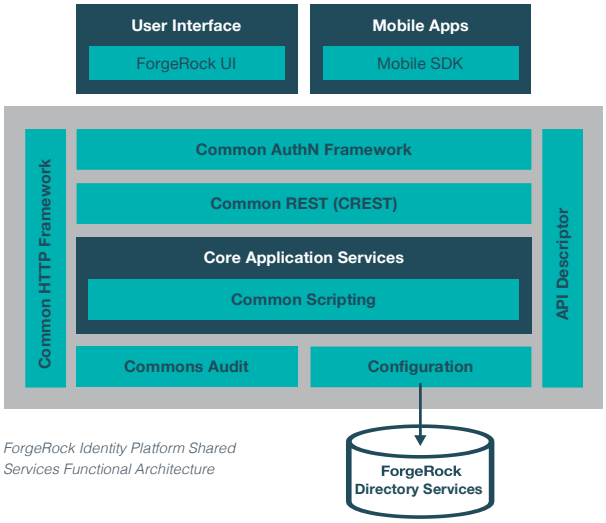
Borderless Over Perimeter

Once upon a time, employees arrived at the office, logged into secure systems, and logged back off at the end of the day. In today's work-from-anywhere culture, employees, as well as partners and customers, need access from laptops, phones, tablets, cars, wearables, and more. They access secure data stored not only on company premises, but also in the cloud and hosted by SaaS providers.

Modular Over Monolithic

Today's IRM demands are much more complex than those of employee-facing IAM. A good IRM solution is designed from the ground up as an integrated, cohesive platform that is purpose-built to handle the complexity of customers and devices. Employee-facing IAM, typically built piecemeal through acquisitions and tacking on parts as needs arise, struggles to respond to the multitude of users, circumstances, devices, access points, and access privileges that dominate today's IRM world.

As more people, devices, and things are assigned identities across networks, IRM services that are simple, flexible, scalable, and designed to quickly verify identities and access privileges become imperative for any business to safely and efficiently engage with their customers. Today's solutions must link devices—laptops, phones, touch pads, cars, wearables—and new mobile and social apps to a single security platform that works all the time, everywhere, on premises or off in the cloud. Our ForgeRock Identity Platform™ is designed with this new reality in mind.



ForgeRock Identity Platform Shared Services Functional Architecture

ForgeRock Model: Shared Platform Services

ForgeRock is committed to the development of trusted identity relationship management through the creation of simple, developer-friendly identity solutions that we call the ForgeRock Identity Platform. A single, common programming interface, provided by ForgeRock Shared Platform Services, enables simple access across the entire platform from access management, identity management, user-managed access, directory services, and an identity gateway. Removing the complexity of the underlying services is a significant advantage to developers and the business. Now for the first time, a developer can utilize reusable shared services across an entire identity platform, whatever the requirements of the application strategy.

This is a completely different model from the standard legacy provider approach, which requires developers to bend applications to support the legacy vendor.

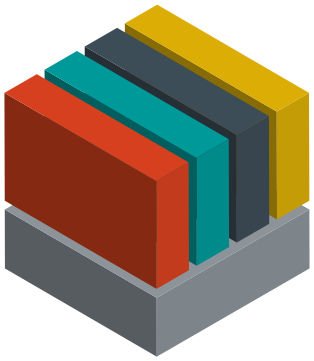
ForgeRock Identity Platform Functional Architecture

ForgeRock Identity Platform

The ForgeRock Identity Platform is a shared services-based architecture, designed to provide a unified experience for developers and administrators in managing the complete life cycle of an identity and its ongoing usage including: the attributes, credentials, and entitlements; the real-time controls for access based on attributes, role, entitlement, and context; and the administration and reporting of those activities. Optimized for scale, these shared services include a common RESTful API, standards-based services such as OAuth2.0, OpenID Connect, SAML and UMA 2.0 among others. Our shared services also have a common lightweight UI model, scripting, logging and high availability to help integrate the ForgeRock Identity Platform components across all identity services as well as external systems. This approach eliminates typical inefficiencies, saving organizations the frustration and time it takes reconciling multiple APIs, UIs, logging, documentation and more.

The ForgeRock Identity Platform consists of the following solutions:

ForgeRock Access Management is a single, unified solution providing advanced authentication, intelligent authentication, mobile push authentication and authorization, contextual authorization, adaptive risk, federation, single sign-on, social sign-on, basic self-service adaptive risk, privacy and consent, high performance and session management, and OAuth2 Proof of Possession all in one self-contained Java application. Built for today's digital challenges, ForgeRock Access Management is designed to give customers not only context-aware single sign-on access, but also a personalized experience via any digital channel, whether a mobile device, connected car, home appliance, or the next connected innovation.



ForgeRock Identity Management provides self-service, provisioning, progressive profiles, social registration, profile and privacy management, password management, synchronization, reconciliation, identity visualization, and a work flow engine, to seamlessly manage identities of people, services and things, whether on premises, in the cloud or in a hybrid environment. ForgeRock Identity Management uses the ForgeRock Identity Connector Framework and Toolkit (OpenICF) to aid development of resource connectors.

ForgeRock User-Managed Access provides developer-friendly, standards based privacy and consent. As a centralized federation authorization architecture, it enables customers and employees to selectively and securely delegate fine-grained access to their data from cloud, mobile and IoT sources. Organizations can build customer trust and unlock new opportunities by empowering users to create valuable data mash-ups with up-to-the-minute accurate feeds of data, including health, smart home, location and other sources. Organizations can leverage this UMA 2.0-standard implementation to add delegation capabilities to entire partner app ecosystems and mitigate the risks of a changing regulatory landscape.

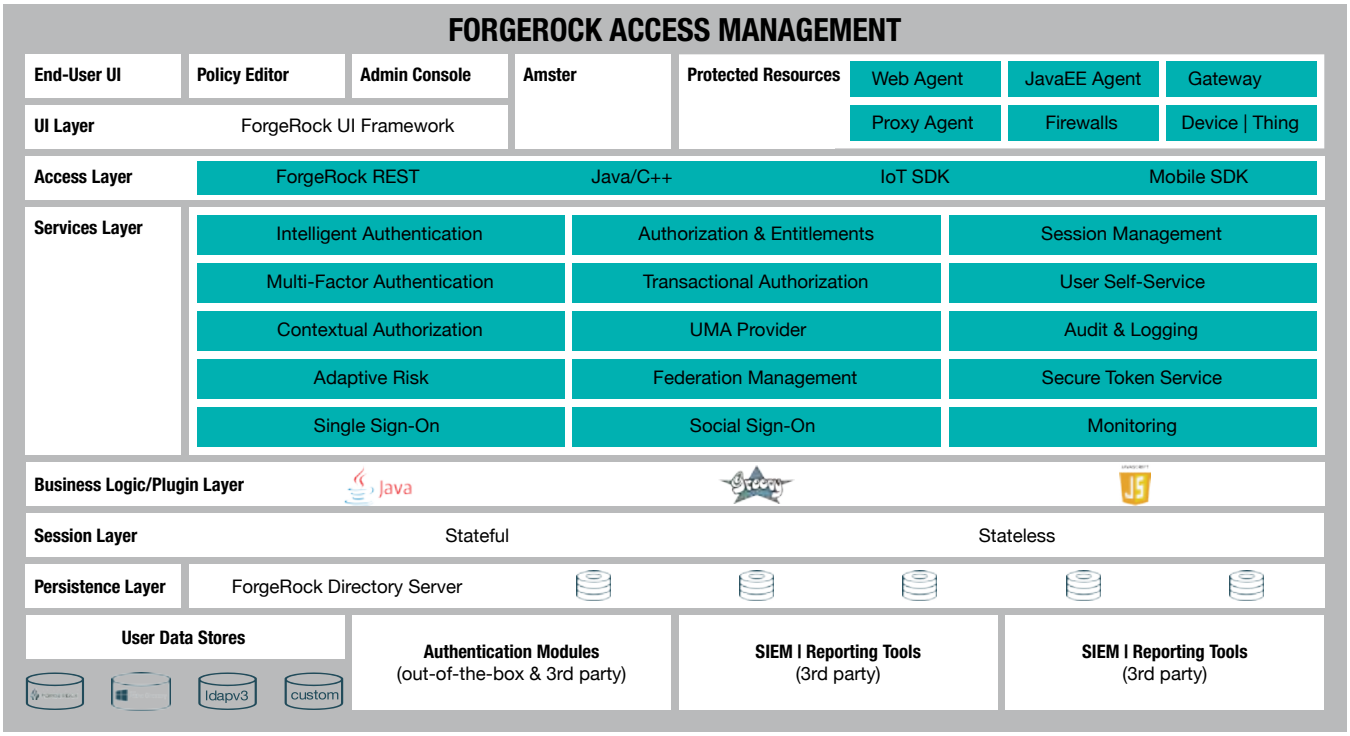
ForgeRock Directory Services provides developers with ultra-lightweight ways to access customer identity data, in order to build a consistent customer profile across the business and personalize services. ForgeRock Directory Services is the first directory server to provide native support for the REST API (application programming interface). It is an LDAP directory service with a high-performance, highly available, secure directory server, built-in data replication, client tools, and a developer-friendly LDAP SDK. Access is provided via LDAP, web services, and REST API.

ForgeRock Identity Gateway extends access to web applications and application programming interfaces (APIs) without recoding. ForgeRock Identity Gateway centralizes identity management for better security consistency, providing one source of truth for who can access what. It intercepts traffic to a resource, ensuring the identity offered is entitled to access the resource requested. A perfect complement to existing web access management systems or as a stand-alone gateway, Identity Gateway provides a flexible policy enforcement point to support your current environment while aiding the migration toward a modern, standards-based platform.

ForgeRock Edge Security offers identity-driven security by creating trusted identities, and ensuring the ongoing authenticity and authorization of connected devices and their transactions or data streams. The Identity Edge Controller provides zero configuration device onboarding, Hardware Root of Trust, issues and manages secure tokens for devices, and more. The Identity Message Broker authenticates and secures data streams from devices.

"Initially, we considered traditional, closed source enterprise IAM vendors to help us drive our vision forward, but it quickly became evident that they would not be able to offer a solution that would be able to integrate or scale as quickly as we needed."

-GREG KALINSKY
Senior Vice President and Chief Information Officer, GEICO



ForgeRock Access Management Functional Architecture

ForgeRock Access Management Overview

Access Management in a Single, Unified Solution

ForgeRock Access Management, part of the ForgeRock Identity Platform™, is a single, unified solution that provides the most comprehensive and flexible set of services required for consumer facing identity and access management as well as traditional access management capabilities.

What legacy identity vendors have traditionally delivered as several different products—single sign-on (SSO), social sign-on, adaptive authentication, strong and mobile authentication, federation, self-service, adaptive risk, web services security, fine-grained authorization, and so on—is delivered by ForgeRock as a single, unified offering. Organizations can use the access control services they need in a centralized way, and simply "turn on" additional services when ready. The solution has a unique architecture to support use cases from complex consumer applications with devices and connected things, to multi-protocol federation, to enabling SSO for cloud systems, to enterprise access control, to securing machine-to-machine solutions using microservices. It is especially well-suited for external, customer-facing access requirements. At the highest level, ForgeRock Access Management consists of a single, self-contained Java application, service components such as stateful or stateless session management, client-side APIs and REST, service provider interfaces to enable custom plugins, and policy agents for web and access policies to protect web sites and web applications.

Organizations with existing internal access management solutions can easily integrate ForgeRock Access Management into their environment through API services or through the token translation service. Maintaining all installation and configuration capabilities within one application vastly simplifies deployment of new internally or externally facing services. In addition, agent configuration, server configuration, and other tasks are simplified so they are repeatable and scalable, making it easy to deploy multiple instances of the solution without additional effort. And with support for DevOps and dynamic cloud architectures, ForgeRock Access Management offers push-button deployment, enabling continuous delivery and elastic deployments that dynamically scale for demand peaks and troughs. The embedded ForgeRock Directory Services eliminates the need to configure a separate directory to support the configuration and user stores; if desired, users can utilize other directories such as Active Directory, DSEE or databases.

4. Privacy in the Digital Era E-Book, Data Sourced from TechValidate

ForgeRock Access Management Key Features

Advanced Authentication

Supporting over 25 out-of-the-box authentication methods, and with the ability to create custom authentication modules based on the JAAS (Java Authentication and Authorization Service) open standard, ForgeRock Access Management enables you to determine the exact conditions in which a resource can be accessed, and to implement strong multi-factor authentication while keeping friction to a minimum. Scripts can be developed and easily integrated to augment authenticity validation by calling, for example, external identity verification systems. Windows IWA is supported to enable a completely seamless, heterogeneous OS and web application SSO environment. And these requirements can be enforced or exempted using the Adaptive Risk capability.

Intelligent Authentication

Intelligent Authentication is based on a powerful authentication tree framework that provides more flexibility, choice and security than traditional authenticators. Identity and security teams can easily configure, measure, and adjust multiple login journeys using digital signals including device, contextual, behavioral, user choice, analytics, and risk-based factors. With an intuitive drag-and-drop interface, you can quickly consume out-of-the-box authenticators, utilize existing authenticators, and integrate with cyber security solutions—all-in-one place. Unlike authentication modules, authentication nodes within trees are more granular and can have multiple outcomes rather than just success or failure. Provide deeper insight into how people and their devices interact with applications and services, improve the end-user experience, deliver dynamic personalization that goes beyond the login journey, and integrate with fraud detection systems to further prevent data breaches.

Mobile Authentication

ForgeRock provides flexible, simple to deploy, and easy to use mobile authentication, seamlessly integrated into the login process. Push Authentication enables secure, passwordless logins and frictionless multi-factor authentication. And one-time passwords provide even more ways to ensure the user is who they say they are. All of this can be implemented using the built-in authentication modules and ForgeRock Authenticator App, available for iOS and Android.

Adaptive Risk

Adaptive Risk is used to assess risks during the authentication process, to determine whether to require the user to complete further authentication steps. Adaptive risk authentication determines, based on risk scoring, whether more information from a user is required when they log in. For example, a risk score can be calculated based on an IP address range, access from a new device, account idle time, etc., and applied to the authentication chain. By using context to evaluate the legitimacy of the user's login attempt, ForgeRock Access Management can bar invalid entrants in real-time.

Authorization

ForgeRock Access Management provides authorization policies, from basic, simple, coarse-grained rules to highly advanced, fine- grained entitlements. Policies can be exported and imported via XACML. By externalizing authorization policy from applications and centralizing it within ForgeRock Access Management, developers can quickly add or change policies as needed, without modification to the underlying applications. Using a modern GUI-based policy editor with its point-and-click, and drag-and-drop operations, sophisticated policies can be built to deliver controlled access to resources. Developers can easily deal with fine- grained policies through REST APIs. For IoT use cases, universal authorization is used where solution-specific policies can be built with arbitrary resource types and custom actions, such as opening a door lock or switching on a light. Most access management solutions only assess risk at initial authentication. Contextual authorization with ForgeRock Access Management, on the other hand, allows for continuous security and dynamic, context-based policies. This allows organizations to assess risk not just at the time of authentication, but also as resources are accessed during the digital session. To gain greater knowledge about who the user is and what their context is, external policy information points can be called with easy to write scripts. Additional context can then be used to further assess risk, requiring stronger authentication mechanisms only when necessary. This makes the end user experience simpler while maintaining security by ensuring the authenticity of people, services, and things throughout the duration of each session. In addition, ForgeRock Access Management can act as a User-Managed Access (UMA) Provider for extensive privacy and consent capabilities, critical in helping to address evolving privacy regulations such as GDPR.

Push Authorization

Enable consumers to securely and conveniently approve high risk transactions and events, via mobile phone notifications. Push authorization provides a first person based approval mechanism that is event based, increases security, and reduces the threat window for malicious activity. For example, an online bank user attempting to transfer money over a critical threshold to an existing payee would would trigger a mobile push notification, which the end user would approve using Touch ID or swipe. If the user attempted the same transaction only seconds later, the same approval would be required, to reduce malicious replay attacks. As more people and things come online, organizations need a simple way to manage them. To date, things like MFA have been primarily an authentication process. ForgeRock makes it an authentication and authorization process.

Federation

The federation services in ForgeRock Access Management can securely share heterogeneous systems or domain boundaries using standard identity protocols (SAML, OpenID Connect). This allows users to access services that span the cloud and mobile devices, on premises and off, eliminating the need for multiple passwords, user profiles, and the added complexity that frustrates users and slows adoption. SAML-based federation can be incorporated into authentication chains, enabling the use of federated identities in stronger multi-factor authentication.

Single Sign-On (SSO)

ForgeRock Access Management provides multiple mechanisms for SSO, whether the requirement is to enable SSO in a single domain, enable cross-domain SSO for a single organization, or enable SSO across multiple organizations through the Federation Service. It supports multiple options for enforcing policy and protecting resources, including policy agents that reside on web or application servers. The built-in Security Token Service (STS) can act as a multi-protocol hub, translating for providers who rely on other, older standards. A variety of flexible options for single sign-on are provided.

User Self-Service

ForgeRock Access Management is an ideal solution for customer-facing identity where it's essential to employ a light touch when dealing with millions of users, all while providing the highest possible security. Businesses need to deliver a great, easy-to-use self-service login, empowering the user wherever possible, such as through easy self-registration or password reset. Otherwise customers are very quick to go somewhere else.

Social Sign-On

ForgeRock Access Management supports social sign-on via social identity providers such as Facebook, LinkedIn, Google, Instagram, VKontakte, and WeChat, allowing users to login directly with their existing social accounts, thus paving the way for rapid customer adoption. In cases where you users should have accounts on your system, the Social Identity module of the ForgeRock Identity Platform can be added, giving full social registration capabilities. This lets users bring registration information such as name, email address, and so on, over from a social provider, significantly shortening registration time.

OAuth 2.0 Proof of Possession & Device Registration

The ForgeRock Identity Platform is an early adopter of the OAuth 2.0 Proof of Possession standard, ensuring that a token presented by a client (for example, a web browser accessing an application, or an IoT

device connecting to a back-end system, and so on) is being presented by its rightful owner. This provides a transparent challenge/response-style interaction to prove the client is the intended owner of the access token and allows organizations to confidently create applications and services to meet their customers' needs, with less concern about token misuse from man-in-the-middle and other attacks.

In addition, device registration or pairing to particular services can be easily set up according to the de facto standard OAuth 2.0 Device Flow, enabling companies to create unique product offerings that incorporate trusted devices and things.

DevOps and Developer Support

ForgeRock Access Management was designed from the beginning for interoperability and massive scale, ideal for customer facing deployments. Today, companies creating new products and services have embraced DevOps to achieve a faster time to market. With its DevOps friendly architecture, ForgeRock Access Management integrates seamlessly into continuous delivery environments, providing a comprehensive set of identity services to help companies generate new revenue streams and set themselves apart from the competition. With ForgeRock Access Management, organizations can leverage automation and orchestration for push-button deployment and continuous delivery.

Additionally, ForgeRock Access Management provides client application programming interfaces with Java and C APIs and a RESTful API that can return JSON or XML over HTTP, allowing users to access authentication, authorization, and identity services from web applications using REST clients in their language of choice. OAuth 2.0 also provides a REST interface for the modern, lightweight federation and authorization protocol. Features such as user self-service, policy, and security token service are also exposed through REST APIs, making it simple for developers to adopt powerful functionality. Widely used in mobile and web applications, OAuth 2.0 and OpenID Connect standards are more rigorously enforced, as the built-in OpenID Connect Provider is fully conformant with the OpenID Foundation's Conformance tests. This ensures greater interoperability and consistent behavior for developers.

High Availability and Scalability

With the advent of IoT, scaling identity systems has become even more challenging. Classic deployment scenarios involve stateful architectures where complex, multi-site failover environments offer extremely high reliability and uptime. And more recently, modern elastic cloud environments have allowed organizations to dynamically scale their production environment to meet demand peaks and troughs. The ForgeRock Identity Platform can do both, with stateless and stateful session architectures that also enable "five 9's" availability for large-scale, mission-critical deployments. Stateless architectures are optimal for deployments with massive scale, into the hundreds of millions, and even billions of identities. With its Docker support and comprehensive remote configuration tools, ForgeRock Access Management is an ideal fit for these dynamic deployments. And for more traditional stateful architectures, ForgeRock Access Management provides both system failover and session failover. These two key features help to ensure that no single point of failure exists in the deployment, and that the ForgeRock Access Management service is always available to end-users. Redundant ForgeRock Access Management servers, policy agents, and load balancers prevent a single point of failure. Session failover ensures the user's session continues uninterrupted, and no user data is lost.

Common Auditing Architecture

The Common Audit Framework provides a means to log data consistently across the ForgeRock Identity Platform, and enables you to correlate events and transactions. Audit topics, such as access and activity, can be configured independently delivering the data you want to the appropriate business services. Handlers are available for Elasticsearch (part of the Elastic stack), JMS, CSV files, JDBC connections, and Syslog.

Customer Use Case: Government of Norway

THE CHALLENGE

Deliver secure government services to Norwegian citizens and businesses so they can do things like obtain birth and death certificates, apply for schools and student loans, manage welfare services and health information, and pay parking tickets, automobile registration fees, utility bills, and taxes online.

THE SOLUTION

Implement a flexible, secure, single-access architecture built with ForgeRock Access Management to enable nearly 100% of all citizens to access over 300 government services.

HOW

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, which 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. Each of the authentication eIDs can be associated with different authentication contexts and different authentication strengths.

BENEFITS

» Nearly 100% of adult citizens and over 500,000 businesses access municipal, regional, and national government services from a single portal online, resulting in ease of use, better security, faster processing times, and measurable savings.

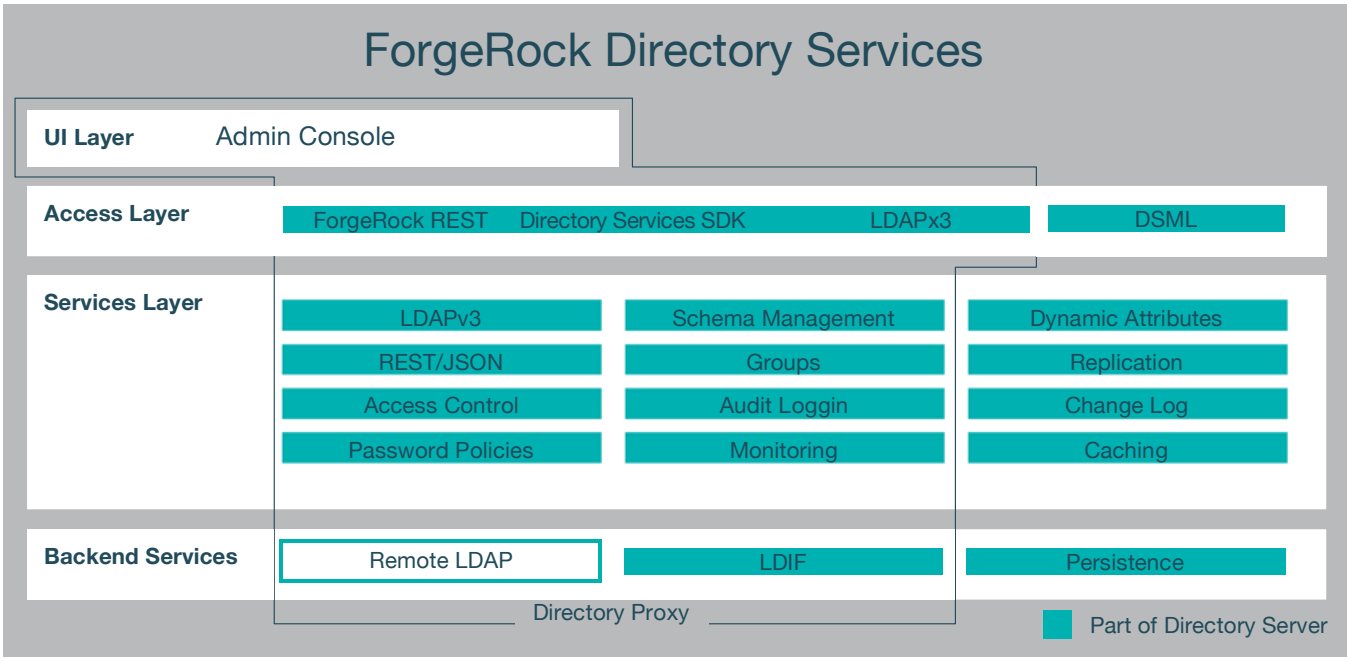
» Scalability and performance: ID-Porten and the authentication environment can handle more than one million users signing in on a single day without outages or degradation in performance, such as on the day taxes are due.

"ForgeRock Access Management's[1] simple, secure access to government services played a large part in the success of the eGovernment initiative."

- TOR ALVIK
COO, Agency for Public Management & eGovernment

Government of Norway

Providing 4M citizens access to
300+ government services online



ForgeRock Directory Services Functional Architecture

ForgeRock Directory Services Overview

Directory Services at Unparalleled Scale

ForgeRock Directory Services, part of the ForgeRock Identity Platform™, is a lightweight, embeddable directory that can easily share real-time customer, device, and user identity data across enterprise, cloud, social, and mobile environments. Core to the management of identity information, ForgeRock Directory Services are used in many different use cases—whether for large-scale cloud service directories, consumer-facing directories, or enterprise or network operating system (NOS) directories.

With an 100% Java code base, ForgeRock Directory Services runs on many platforms, including virtualized environments. All software and data are architecture-independent, so migration to a different OS or a different server is as simple as copying an instance to the new server. This increases the deployment flexibility, as well as the portability between different operating systems and system architectures.

Recognizing the complexity of traditional identity data access, ForgeRock Directory Services provides developers with new options. Developers no longer need to be LDAP experts. ForgeRock Directory Services lets developers choose either LDAP or REST to access identity data, using a single solution that can replicate data across on-premises and off-premises applications. ForgeRock Directory Services combines the security of a proven directory with the accessibility of a database.

ForgeRock Directory Services Key Features

Large-scale Performance, Data Integrity, and Security
ForgeRock Directory Services is optimized for performance at scale with data integrity and security. With millisecond response times and read/write performance in the tens of thousands per second, ForgeRock Directory Services satisfies the most rigorous performance requirements across industries, from telecom and financial services to large-scale consumer-facing applications. Directory Proxy extends horizontal scalability in multi-tenant environments, providing even more availability, performance and better security for distributed architectures. And, simplifies change by directing all applications to a single-entry point, eliminating otherwise time-consuming application tuning as directory services requirements expand with digital business needs.

Data Integrity and Security

ForgeRock Directory Services stores identity data securely, with varying levels of authentication and authorization, including SSL, StartTLS, and certificate-based. Password and data encryption provide enterprises the means to securely deploy directory services on public clouds or use shared file systems infrastructures. The encryption ensures the confidentiality and integrity of the data at rest which adds a critical layer of security from malicious attacks and potential breaches. All configuration changes are audited and archived, offering easy rollback to a working configuration. Businesses can have confidence in a service that will scale well beyond their business requirements.

Replication Services to Guarantee Data Availability
By replicating data across multiple directory server instances, key customer, device, and user data is preserved in case of an outage. ForgeRock Directory Services provides advanced replication options including multi-master, fractional, and assured. N-Way multi-master replication provides high-availability and disaster recovery capabilities. Fractional replication enables only specific attributes to replicate. Assured replication can guarantee data availability even in the remote scenario of a server crash. ForgeRock Directory Services also offers advanced backup and restore functions such as automated, compressed, signed, and encrypted backups that improve data reliability and security. Administrators can take advantage of the easiest replication setup in the industry to ensure a consistent data store and data availability across the organization.

Delegated Authentication Without the Security Risks of Password Synchronization

ForgeRock Directory Services permits delegated authentication to another LDAP directory service, such as Active Directory, with pass-through authentication. Pass-through authentication removes the security risks associated with synchronizing passwords (including possible capture and transfer of clear text passwords). With pass-through authentication, ForgeRock Directory Services replays a user's simple bind operation against the remote directory service. If the bind is successful, ForgeRock Directory Services considers the user authenticated to perform subsequent operations like searches and updates in ForgeRock Directory Services. IT organizations can leverage pre-existing investments in services like Active Directory to deliver secure identity across disparate systems.

Monitoring to Inform Administrators About Directory Service Events

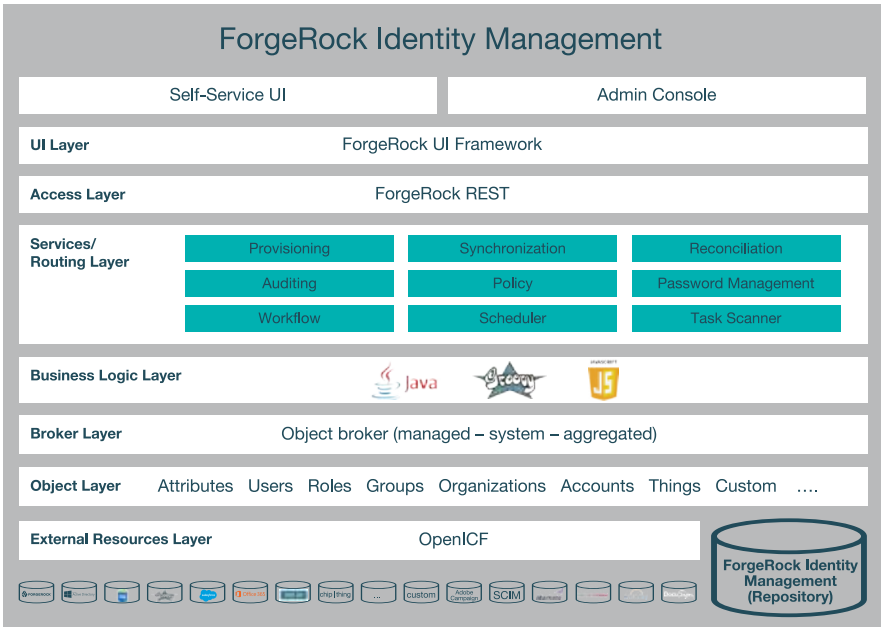
By supporting the widely-adopted monitoring standards SNMP and JMX, ForgeRock Directory Services can easily integrate into your existing monitoring infrastructure. Configure custom alerts to inform administrators about specific directory service events, such as password expiration, account lockout, backend database corruption detection, and much more. IT organizations get a transparent view into the status and performance of the directory.

Advanced Developer Access and Administration to Simplify Installation and Server Configuration

ForgeRock Directory Services installer simplifies installation and server configuration down to a few minutes. The command line utilities enable complete access to all server management controls and monitoring, locally or remotely. ForgeRock Directory Services provides data access through multiple protocols: REST, LDAP, and Web Services. It fully complies with LDAPv3, and DSMLv2 standards to ensure maximum interoperability with client applications. ForgeRock Directory Services SDK provides a high-performance, easy-to-use library of classes and interfaces for accessing and implementing LDAP directory services. Administrators can leverage existing expertise to enhance and deploy ForgeRock Directory Services without the need for external services.

Common Auditing Services

The Common Audit Framework provides a means to log data consistently across the ForgeRock Identity Platform, including ForgeRock Directory Services, and enables correlation of events and transactions. Audit topics, such as access and activity, can be configured independently delivering the data you want to the appropriate business services. In addition to the existing handlers for csv files, jdbc connections, and syslog, and Elasticsearch (part of the ELK stack).



ForgeRock Identity Management Overview

Identity Lifecycle Management for People, Services and Things

ForgeRock Identity Management, part of the ForgeRock Identity Platform™, is built from the OpenIDM and OpenICF open source projects, and is an identity administration and provisioning solution focused on managing relationships across people, services, and things, designed in response to the pain organizations suffer deploying legacy enterprise provisioning solutions. These mostly proprietary solutions are monolithic, heavyweight, painfully slow to deploy, and outrageously expensive; furthermore, they are not prepared for today's organizational needs, like connecting to cloud infrastructure and internet-connected devices and things.

Unlike legacy identity management solutions, ForgeRock Identity Management is a modular, plug-and-play identity service so you consume only what you need. In addition, it has a well-defined and simple REST API that is ideal for anyone in need of provisioning across enterprise, cloud, social, and mobile environments.

Utilizing a Java-based architecture that is built on the OSGi framework and therefore (See ForgeRock Identity Management Architecture) is able to provide lightweight, modular services such as automated workflow, user self-service, profile and privacy management, social registration, progressive profiles, password sync, data reconciliation, and audit logging, all accessible through developer-friendly REST APIs, using standard Java development tools such as Eclipse, NetBeans, Spring, etc.

ForgeRock Identity Management provides multi-layered provisioning activities through an embedded workflow and business process engine based on Activiti and the Business Process Model and Notation (BPMN) 2.0 standard. The modular design enables complete flexibility to use the embedded workflow engine and a database or replace these technologies with your selected platforms and services. Designed to have a small footprint, the entire service can itself be completely embedded and custom-tooled to the requirements of the target applications or services. Manage all of your identity sources: external systems, databases, directory servers, and other sources of identity through the built in identity connector framework, eliminating the need to rip and replace data stores.

Historically, the reason for building an internal enterprise user administration and provisioning system was to connect to the HR system. Now, organizations can support both internal employee systems and large-scale customer-facing applications. Configure the solution to create a virtual identity with links to external systems (data sparse model) or to create a meta-directory that centrally stores (data full model) a copy of identity attributes including virtual links to other external systems.

Key Features

Self-Service to Reduce Friction and Drive Customer Engagement

Being able to provide an easy, seamless registration, login, and password management service to end users is crucial for customer acquisition and retention. Self-service significantly reduces helpdesk costs and improves the customer experience by automating registration and password reset for millions of users. This enables admins to onboard and maintain customer and employee accounts with zero input and little customization required.

Profile & Privacy Management Dashboard–Build Customer Trust and Evolve with Regulations

Meet consumer demand and comply with continually evolving regulations with a transparent and centralized profile management solution. The Profile & Privacy Management Dashboard provides customers self-service for managing their personal info, password, communication preferences, including the option for account deletion. Customers can also manage what personal data is shared with an external database, such as marketing automation platforms. Admins can also track and manage multiple versions of Terms & Conditions, or Terms of Service (ToS), and automatically prompt customers for their consent upon login when a ToS is updated. When combined with ForgeRock Access Management, the dashboard can be used to manage paired devices, applications, shared resources, and monitor activity changes made to the account.

Progressive Profiles

Customers prefer to share small amounts of information at a time. With Progressive Profiles, customers can register using simple, automated forms that progressively gathers information during designated moments of their journey. Easily build forms, gather additional profile attributes asynchronously, and enrich user profile data using automated policy-based rules. It's quick and easy for customers, and helps you gather more relevant, and accurate first party data.

Social Registration & Authentication

Accelerate and simplify registration and login by integrating social IdPs that supports OpenID Connect or OAuth 2.0, and non-standards based IdPs such as Facebook, Google, LinkedIn, Amazon, WordPress, Yahoo, Microsoft Live, Twitter, Instagram, Salesforce, WeChat, and VKontakte. This improves customer experience and helps you to build common user profiles for a centralized single view of the customer. By streamlining the registration and authentication process and consolidating social profiles customers can conveniently use the same identity across applications and devices—a frictionless user experience for your customers. Within ForgeRock's Identity Management, developers can use simple configurations to quickly define scopes and gather specific user data for deeper insight into your customers.

Password Synchronization for Enforcing a Secure, Centralized Password Policy

ForgeRock Identity Management password synchronization, is a service that allows organizations to synchronize passwords in real time to ensure uniformity across all applications and data stores such as Active Directory. With password synchronization, any user, device, or connected thing authenticates using the same credentials on each resource.

Provisioning Based on Custom-Tailored Workflows

Leverage ForgeRock's Identity Management workflow and business process engine to create, read, update, and delete functions based on workflow-driven provisioning activities. Add workflows for self-service actions such as a user or device requesting access to an application, or an administrator handling bulk onboarding or off-boarding. To simplify defining workflows and business processes, the embedded Activiti module can be used for modeling, testing, and deployment. Activiti is based on the standard BPMN 2.0 process definition models, which can not only exchange between different graphical editors, but can also execute as is on any BPMN 2.0-compliant engine. Organizations can easily custom- define workflows and business processes that meet their unique needs.

"When it comes to identity management, legacy systems were not built with the modern world in mind. They were built for on-premises employees using a company-provided computer. As times have shifted to a multi-device-owning, always- connected mobile workforce, the complexity, cost, and potential for vendor lock-in of these legacy solutions has become increasingly apparent."

- ESG LAB VALIDATION
ForgeRock Identity Platform

ForgeRock User-Managed Access Overview

Centralized delegation that empowers consumers and businesses to share and unlock new data potential across cloud, mobile and IoT sources.

User-Managed Access (UMA) is an OAuth-based access management protocol standard designed to give an individual a unified control point for authorizing who and what can get access to multiple sources of digital data, content, and services. UMA's federated authorization architecture is non-proprietary and resolves a host of access control, privacy and consented sharing issues in today's API and IoT economies. ForgeRock User-Managed Access is part of the ForgeRock Identity Platform, and is the world's first consumer-facing, unified implementation of the UMA standard. It enables a strategic response to a changing regulatory landscape while enabling robust application, mobile, and device ecosystems. ForgeRock's VP of Innovation & Emerging Technology, Eve Maler, founded and chairs the UMA standards effort and also cofounded and co-chairs the Health Relationship Trust (HEART) standards effort that is profiling UMA (along with OAuth, OpenID Connect, and the FHIR API) for patient-centric health data sharing.

UMA gives your customers and employees a convenient way to determine who and what gets access to personal data, for how long, and under what circumstances, which is especially important in the era of GDPR and other data privacy regulations that prioritize choice and control for data subjects. The UMA 2.0 standard includes an extension grant of OAuth 2.0 and has additional simplicity, security, and internet of things benefits.

UMA Provider Key Features

Fine-Grained Delegation and Consent
Gives end users a convenient central console for organizing digital resources residing in many locations, delegating scoped access to others, and monitoring and revoking access.

Fine-Grained Access Denial
Provides a dedicated landing page for aggregating pending access requests; the end user can grant requests, edit down the scopes granted, and deny requests outright.

Chained Delegation
Enables a resource requester to re-share it with another requester; the original owner can see the entire access history and disrupt the sharing chain by revoking the original policy.

Dynamic Resource Protection Onboarding
Enables each data service to put their digital resources under central protection as the resources are created and changed.

Security Controls and Usability Features
Lets an administrator set realm-level features such as access token expiration times and email notifications surrounding pending access requests.

Customizability
Lets implementers use extensive API endpoints and plug-in points to customize just about any characteristic of the UMA Provider, including replacing the standard XUI interface for the console.

User-Managed Access (UMA) Standard
Provides conformance to the UMA standard for industry interoperability and easy application of the ForgeRock solution framework to your entire organizational or partner ecosystem, including federated authorization use cases as well as customer-centric use cases.

"Serving the needs of citizens in New Zealand in an efficient, privacy-preserving way calls for a customer-centric approach to access control and the tools to match. For example, students might want to share authoritative records of achievement with career advisors and potential employers. We are therefore currently undertaking a proof of concept to explore UMA as a scalable standard that can help citizens interact with government more efficiently and conveniently."

- ESG LAB VALIDATION
ForgeRock Identity Platform

UMA Protector Key Features

Multi-Service Protection Gateway
Provides an enforcement point over any number of data services or APIs, so that multiple UMA resource servers to which the resource owner has login accounts can be protected by the authorization server.

Requester Trust Elevation for Increased Security
Ensures that access requesters aren't just in possession of a "secret link" but requires them to prove they are who they say they are, according to resource owner policy.

Dynamic Policy Enforcement Point Onboarding
Lets your web API register its digital resources with an UMA authorization server as those resources are created and changed.

User-Managed Access 2.0 Standard
Provides conformance to the UMA 2.0 standard (OAuth extension grant and federated authorization) for industry interoperability and easy application of the ForgeRock solution framework to your entire organizational or partner ecosystem, for applicability to customer-centric use cases.

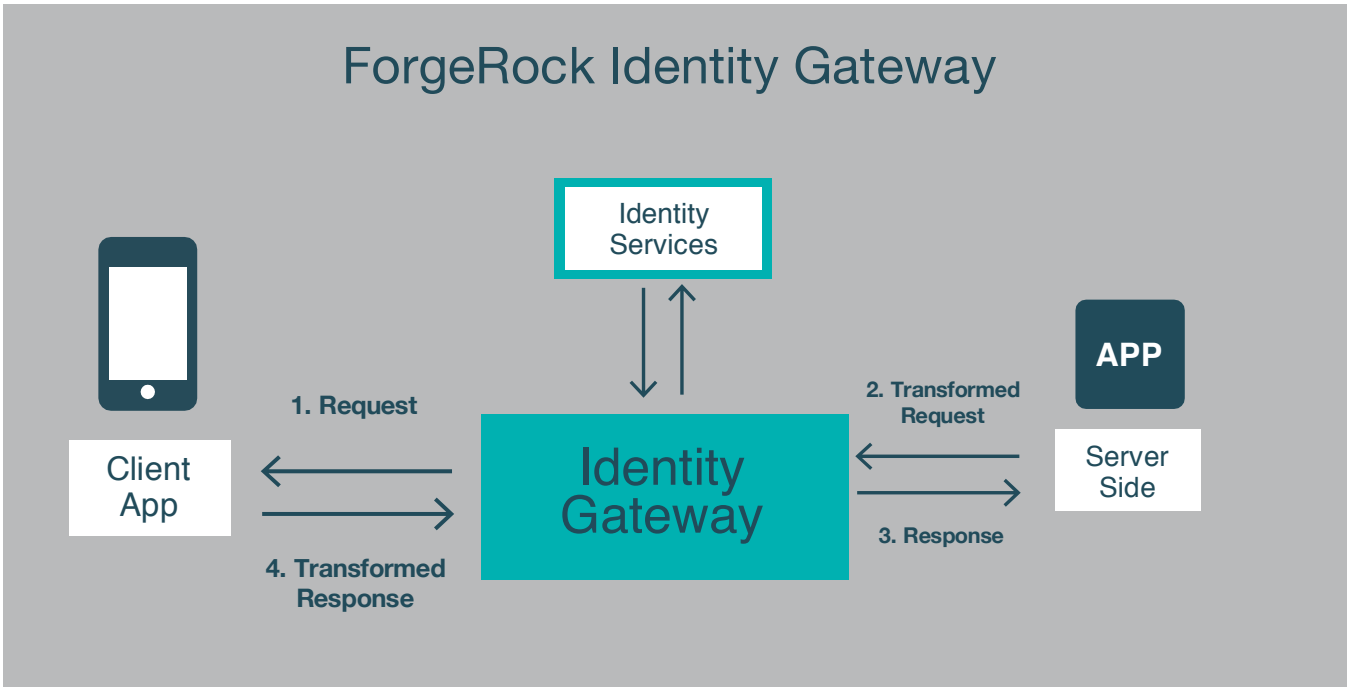
"At Philips, we're on a mission to improve people's lives and to empower people to take better care of themselves and others. With the rise of cloud-based data, health and wellness apps and consumer sensors, it's important to be able to share all those sources of data with family members, health professionals and others under close personal control," said Jeroen Tas, CEO, Healthcare Informatics Solutions and Services, Philips. "With UMA, we are able to design innovative data-sharing and consent technologies into our HealthSuite Digital Platform that make it possible to foster consumer and patient trust."

- JEROEN TAS
CEO, Philips

ForgeRock Identity Gateway Overview

Centralized identity gateway for applications, devices, & things
ForgeRock Identity Gateway is an incredibly lightweight, flexible and high performance identity gateway that can provide identity services to any web traffic. Part of the ForgeRock Identity Platform™, the ForgeRock Identity Gateway is, in its simplest form and most basic configuration, a Java-based reverse proxy that runs as a web application. It routes all HTTP web traffic to protected applications through a centralized gateway, verifying the validity of messages, enabling the close inspection, transformation and filtering of each request. In simpler terms, ForgeRock Identity Gateway checks the identity of web traffic as it passes through, stopping those without permissions and letting the rest pass. By enforcing rules, it can determine who, what and when access is allowed to which resource.

Acting as a bridge between legacy and or modern web applications and the identity management platform, the ForgeRock Identity Gateway enables IT to transition the identity integration of the app from legacy to modern. The Identity Gateway identity-enables any target application via OAuth2, OpenID Connect or SAML2. The token transformation and password replay capabilities bridges identity to how the application requires – without installing anything with the target application.



ForgeRock Identity Gateway Functional Architecture

ForgeRock Identity Gateway Key Features

Single Sign-On and Sign-Out

Improves User Experience. ForgeRock Identity Gateway reduces the proliferation of passwords and ensures consistent, secure access across multiple web apps and APIs. The ForgeRock Identity Gateway can leverage any standards-compliant identity provider to integrate into your current architecture. Single sign-on and sign-off improves the user experience and will vastly improve adoption rates and consumption of services provided.

Authorization Enforcement Security

ForgeRock Identity Gateway can authenticate all traffic passing through the gateway, adding a valuable layer of security. The solution leverages OAuth 2.0 and OpenID Connect for securing access to API end-points that are exposed externally. ForgeRock Identity Gateway is often deployed in the DMZ, as it has traffic-routing capabilities that send web traffic to the correct internal resources. The ForgeRock Identity Gateway reverse proxy functionality enables an agentless architecture, eliminating the need for agents on each individual internal resource, and augmenting existing web access management (WAM) deployments. When all traffic goes through a gateway, administrators can ensure that all traffic identities are authenticated, providing an additional layer of security. And a powerful design studio lets developers configure Identity Gateway, only once, into a test or production environment.

Organizations can balance security and a frictionless user experience with context-based authorization ForgeRock Identity Platform extends contextual authorization across the platform to Identity Gateway, increasing the security of resources by enabling organizations more ways to capture context and evaluate whether stronger or simpler authentication is needed. Identity Gateway helps organizations balance security and a frictionless user experience.

Throttling, Monitoring and Auditing Adds Security

Prevent unwanted traffic from disrupting operations and uphold SLA's with ForgeRock Identity Gateway's throttling functionality, ensuring apps give the right access without having to worry about DDoS attacks. ForgeRock Identity Gateway can throttle traffic to increase the security of protected Web APIs and applications. The solution can set limits in terms of transactions over a specific period of time - per second, per minute, per hour, per day, per week etc. Specify per user, domain name, IP address or based on different classes of applications or users, for example throttle based on subscription level like gold, silver, or bronze. Monitor and Audit traffic passing through the ForgeRock Identity Gateway to enable alerting and reporting of events.

Throttling, Monitoring and Auditing Adds Security

Prevent unwanted traffic from disrupting operations and uphold SLA's with ForgeRock Identity Gateway's throttling functionality, ensuring apps give the right access without having to worry about DDoS attacks.

ForgeRock Identity Gateway can throttle traffic to increase the security of protected Web APIs and applications. The solution can set limits in terms of transactions over a specific period of time - per second, per minute, per hour, per day, per week etc. Specify per user, domain name, IP address or based on different classes of applications or users, for example throttle based on subscription level like gold, silver, or bronze. Monitor and Audit traffic passing through the ForgeRock Identity Gateway to enable alerting and reporting of events.

Password Capture and Replay Simplifies Support of Legacy Web Applications

Using the ForgeRock Identity Gateway, organizations can add a layer of identity security to applications and APIs without costly and time-consuming changes to each individual app. ForgeRock Identity Gateway is even able to look up usernames and passwords in a legacy database and replay them to the web app or API. By reducing the number of passwords end-users need to remember, IT can reduce the costs of maintaining legacy applications.

WAM Policy Agent Management Simplified

In cases where policy agents are available for applications, there may be too many to easily deploy, especially if you have hundreds or thousands of web apps and limited resources to test and manage them. The ForgeRock Identity Gateway is a centralized enforcement point without the policy agent overhead. Administrators can reduce the time required to manage web apps by leveraging a single gateway.

Message Transformation Acts as Translator

ForgeRock Identity Gateway can transform messages passing through the gateway, adding and removing headers and other variables that would otherwise prevent one type of system from communicating with another in a standards-compliant manner. This allows administrators to shape the traffic an app receives, or even to split the traffic between multiple web apps or APIs, virtualizing the endpoint and streamlining the integration capabilities of the current infrastructure.

SAML-Based Fedlet Simplifies Federation

ForgeRock Identity Gateway makes federation less complicated by including the ForgeRock Access Management Fedlet—a small web application that can act as a Service Provider—in order to quickly and easily add a SAML end-point to your environment.

Standards-Based Solution Has Simple Setup and Configuration

ForgeRock Identity Gateway supports JWT sessions, as well as SAML, OAuth 2.0, UMA 2.0 and OpenID Connect for easy integration between SaaS, cloud, and mobile services, in addition to on-premises infrastructure. This gives the ForgeRock Identity Gateway a great deal of deployment flexibility, supporting any third-party WAM solution or existing web app environment. ForgeRock Identity Gateway is also designed for easy, step-by-step configuration--it's simple to read the configuration files with inlining and decorators. In addition, ForgeRock Identity Gateway can quickly activate dynamic logging and debugging information. Administrators can leverage existing expertise to enhance and deploy Identity Gateway without the need for external services.

Common Auditing Services

The Common Audit Framework provides a means to log data consistently across the ForgeRock Identity Platform, including ForgeRock Identity Gateway, and enables correlation of events and transactions. Audit topics, such as access and activity, can be configured independently delivering the data you want to the appropriate business services. In addition to the existing handlers for csv files, jdbc connections, and syslog, and Elasticsearch (part of the ELK stack).

> ***"Application investment and upgrades are driven purely by retail business needs, not by IT. Outside of a gateway, the only way we can get apps updated with identity is if there is an active project to upgrade it."***
>
> - FORTUNE 500 RETAILER
> Describing their legacy app estate and identity challenges

loud Foundry Route Service

Simply put, many microservices and applications do not come with security built-in and developers must write and rewrite identity capabilities into each application and service. With the use of Route Services, applications and microservices security can be externalized using the extensive capabilities of the ForgeRock Identity Platform as a centralized Identity solution across all applications.

DevOps Friendly

DevOps isn't new. It's been helping developers and IT operations work more efficiently together to tackle the demands that innovation is constantly slinging at them. And with Identity at the center of everything, it's important that your identity platform is a well-oiled, push button delivery point for proper DevOps collaboration. The ForgeRock Identity Gateway is

a perfect fit for DevOps environments. ForgeRock Identity Gateway embraces DevOps methodology by using container-oriented technologies such as Kubernetes and Docker for rapid automation of deployments. Further, it sits with the application and scales as the application scales, allowing continuous integration and increasing the speed of change from development to production.

"A key reason Spark NZ chose the ForgeRock Access Management solution was for its ability to integrate with legacy web applications. Identity Gateway—a high-performance reverse proxy server with specialized session management and credential replay functionality. ForgeRock Identity Gateway works together with Access Management to integrate web applications without the need to modify the target application or the container that it runs in—delivering significant cost- savings. With time and budget considerations for such a large IT project, the ability to quickly and easily integrate with existing applications was critical to the overall success of the project."

- SPARK NZ CASE STUDY

ForgeRock Edge Security Overview

Secure Edge Devices for the IoT

The internet of things (IoT) is revolutionizing industries with connected devices creating a complex web of captured data. These connected devices can streamline processes and allow companies to create innovative operational architectures, but it is not without risk. As systems begin to operate autonomously with automated decisions, it is necessary that IoT devices are trusted and their data is secured. If an automated system is fed incorrect data, whether innocently through simply misidentifying a device, or with bad intentions through falsification, the whole integrity of the system is compromised. This is where ForgeRock Edge Security comes to the rescue.

ForgeRock Edge Security offers identity-driven security by creating trusted identities, and ensuring the ongoing authenticity and authorization of connected devices and their transactions or data streams. Combined with the existing ForgeRock Identity Platform, the new capabilities support highly trusted authentication and granular relationship-based authorization decisions for common IoT design patterns, including device-to-device, device-to-service (i.e. cloud and/or microservice), and user-to-device, among others.

ForgeRock Edge Security can help you close the IoT security gap and build a foundation for trusted identity relationships with a secure solution that includes contextual security, open standards, and IoT-grade scalability.

ForgeRock Edge Security Key Features

Identity Edge Controller

The Identity Edge Controller (IEC) runs on smart edge devices, providing edge privacy and integrity, including secure device attestation. With a broad range of deployment options, even where network access is not always guaranteed you can ensure trusted relationships between devices at all times. IEC also enables devices to harness further capabilities of the platform such as standards-based tokens, authentication, and authorization between devices,

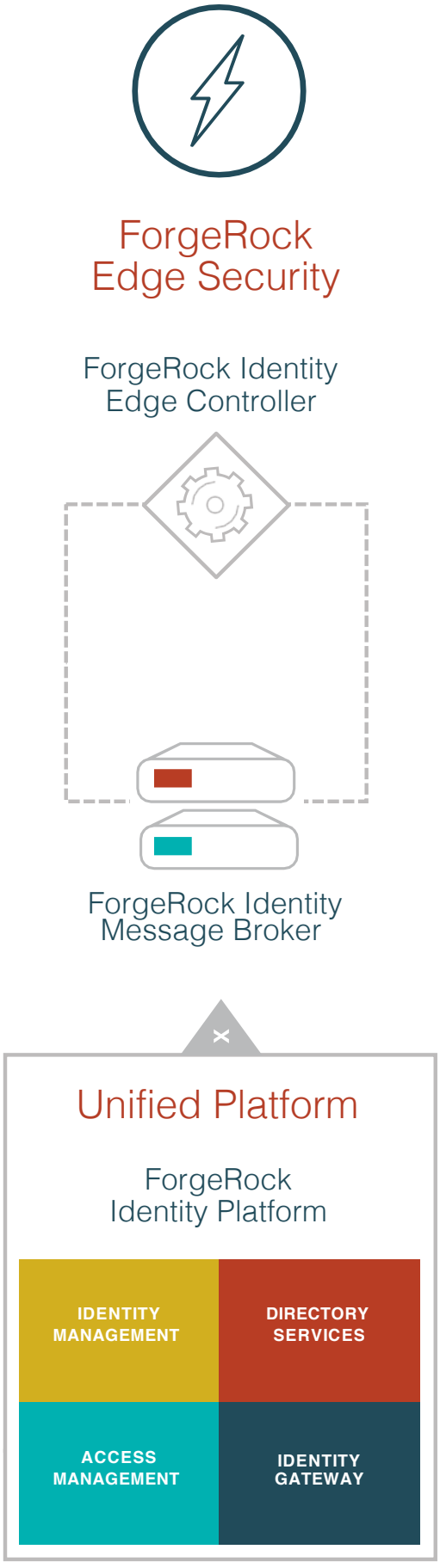
and between devices and other cloud or distributed microservices. Features include, secure device attestation and on- boarding of trusted device identities, device authentication and authorization, proxied on-boarding of simple and constrained edge devices secure configuration endpoints for connected devices and services, and root of trust-based signing and encryption.

Identity Message Broker

Organizations today need a way to secure and identity-enable industrial IoT data flows that don't speak HTTPS. Unfortunately, many IoT data flows using popular protocols like MQTT (Message Queuing Telemetry Transport) lack secure authentication and authorization.The Identity Message Broker compliments the device security provided by the Identity Edge Controller by providing message-level security over native IoT protocols. The Identity Message Broker installs on-premise, in the cloud, or on the edge, and can receive data streams from thousands of IoT devices. It authenticates the source and secures the data, and authorizes data flows. The Identity Message Broker can even be configured to install on the same hardware as the Identity Edge Controller, providing an all in one IoT edge security solution. Features include authentication and authorization enforcement for MQTT that secures and hardens the sending and receiving of MQTT dataflows between an edge client and the cloud in Internet of Things (IoT) systems. Token-based validation of devices also enables revocation and expiration of credentials, ensuring device identity.

Conclusion: The ForgeRock Advantage

The ForgeRock Identity Platform provides a vibrant alternative to traditional employee-facing IAM platforms. The ForgeRock Identity Platform is developer-friendly for building identity relationship management services for enterprise, cloud, social, and mobile systems. The ForgeRock Identity Platform enables agile business innovation with its modular, massively scalable, and lightweight infrastructure. For technical staff, the ForgeRock Identity Platform provides a simple, easy-to-use approach to delivering identity services. For CEOs and business line managers, it provides a new, highly effective, and repeatable method of managing relationships with their customers—relationships that are tied directly to the business' top line.



How The ForgeRock Identity Platform Provides Technical Value

ForgeRock is the only unified identity relationship management platform available on the market today. ForgeRock is the first to offer an agile, all-in-one, unified platform for rapidly building customer-facing identity services that are lightweight, modular, massively scalable, and developer-friendly. The ForgeRock Identity Platform is built from the ground up to work as a cohesive whole and connect enterprise, cloud, social, and mobile security strategies into a single, common platform to maintain enterprise-level security. Our platform does this by providing:

- Faster time-to-market: Roll out new identity-enabled services faster than the competition, in weeks and months instead of years.
- Increased Economies of Scale: With a solution that is flexible, repeatable, and scalable for millions of people, things, and applications, businesses can quickly eliminate customer identity silos across the organization, providing cohesive, informed, and secure customer relationships.
- Massive reach: The ability to roll out new identity-enabled services to hundreds of millions of users without fear of bottlenecks or platform limitations.
- Unified Platform: Works as an efficient, cohesive whole to adapt to the internet of things, able to secure employees, partners, customers, and their devices from anywhere, at any time, whatever the circumstances.
- New digital channels: Delivering a unified identity platform with a single, repeatable way for developers to identity-enable new digital services fast makes it easy to accommodate the rapid changes that come with digital transformation.
- Smarter security: Reduce security risks, unauthorized access, and suspicious behavior with proactive security measures that use real-time context, giving you confidence that your most valuable assets—your customers—are protected.

/HIGHLIGHTS

The ForgeRock Identity Platform empowers organizations to achieve their business goals:

- 88% deployed in less one year
- 70% achieved payback in less than 18 months
- 51% improved security & management of user identities
- 41% consolidated customer identity data onto one platform
- 39% increased scalability to support more customer users

Source: TechValidate survey of ForgeRock customers

How The ForgeRock Identity Platform Provides Business Value

The ForgeRock Identity Platform allows businesses to rapidly identity-enable new cloud, mobile, and IoT services in order to offer a richer, seamless customer experience across applications, devices, and internet-connected things. We do this by:

- Consolidating identity platforms across all business units to create a common identity platform companywide. Businesses can get to know their customers better with consistent customer profiles across all business units, arming them with the data to develop new and more meaningful services based on behavior.
- Implementing a digital identity-centered ecosystem that allows businesses to use identity data and real-time context to personalize the customer experience.
- Using real-time context and data insight to protect against malicious digital access, even when passwords have been compromised.
- Giving customers easy access to secure applications where they can buy services, contributing directly to business' top-line revenue.
- Supporting user privacy standards such as User-Managed Access (UMA), which help enterprises address emerging data protection regulations such as GDPR and data residency requirements.

/ABOUT FORGEROCK

ForgeRock®, the leader in digital identity management, transforms how organizations build trusted relationships with people, services, and things. Monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, Open Banking, etc.), and leverage the internet of things with ForgeRock. We serve hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, and Pearson, as well as governments like Norway and Canada.

www.forgerock.com