FORGEROCK® USER-MANAGED ACCESS

DATASHEET

Secure Delegated Authorization that Builds Privacy, Consent and Trusted Relationships

Privacy regulations, like General Data Protection Regulation (GDPR), impact all organizations holding personally identifiable information. Void of compliance, organizations can suffer disastrous repercussions in the form of enormous fines and even imprisonment of executives. Further, lax privacy practices can cost an organization reputation and ultimately consumer trust. But new regulations don't have to bring only doom and gloom. Savvy businesses can leverage these regulations as a way to build trust with their customers. Organizations can opt for a contextual privacy methodology which takes the burden away from the business and puts it into the hands of the consumer - ultimately building trusted relationships necessary for successful digital transformation.

When it comes to customer trust, it's not enough for you to scrape by with bare data protection compliance and opt-in consent forms. And when it comes to business agility and scalability, building your own proprietary end-user data delegation infrastructure and consent tools simply won't do. The amount of data and the number of sources it comes from are growing rapidly; sources include not just web and mobile applications but now connected devices, too. The pressure is increasing for organizations to secure customer data, address privacy regulations going forward, and find ways to use data as a business asset to develop new digital offerings. To unlock exciting new value from cloud, mobile, and IoT sources while building trust into your customer data management, you must build context, control, choice, and respect into every offering – or your customers will seek out your competitors.

HIGHLIGHTS

- End-users can grant, monitor, deny, approve and revoke digital consent.
- Consent can be granted ahead of time ("Share") and after access is requested.
- End-users manage sharing settings from a single centralized console.
- Add delegation capabilities to entire partner app ecosystems and mitigate the risks of a changing regulatory landscape.
- Authorization decisions are as fine-grained as the protected APIs' scopes.

Part of ForgeRock Identity Platform™, ForgeRock® User-Managed Access (UMA) is a standards-based privacy and consent solution that 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. Users delegate access through a simple "Share" button in your app, and can monitor and manage sharing preferences all through a central console. Organizations can build customer trust, overcome privacy and consent challenges, and create new revenue opportunities by empowering users to create and share valuable data mashups with up-to-the-minute accurate feeds of data, including health, smart home, location, and other sources.

What is UMA?

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 resolves a host of access control, privacy and consented sharing issues in today's API and IoT economies.

Features	Benefits
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. 100% Java-based server is extremely efficient with minimal CPU, and on-disk footprint, significantly reducing data center costs.
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 an end user who owns a resource to share it with another, who can in turn share it with another; the original owner can see the entire access history and disrupt the sharing chain by revoking the original policy.
Dynamic Policy Enforcement Onboarding	■ Enables each service used by an end user put their digital resources under central protection as the resources are created and changed. ■ Lets your Web API register its digital resources with an UMA authorization server as those resources are created and changed. Includes a wide variety of password encryption schemes and customizable rules for password strength enforcement to ensure no app can store insecure passwords.
Security Controls and Usability Features	■ Administrators can set realm-level features such as access token expiration times and email notifications surrounding pending access requests.
Customizability	■ Implementers can 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.
Multi-service Protection Gateway	■ Provides an enforcement point over any number of services or APIs, so that multiple UMA resource servers to which the end user has login accounts can be protected by the authorization server.
Requester Trust Elevation	■ Ensures that access requesters aren't just in possession of a "secret link" but goes above and beyond OAuth 2.0 in proving requesters are who they say they are, according to resource owner policy.
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.

> "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
Healthcare Informatics Solutions and Services, Philips

About ForgeRock

ForgeRock® is the Digital Identity Management company transforming the way organizations interact securely with customers, employees, devices, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, FCC privacy, etc.), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA, and Asia.

Get free downloads at www.forgerock.com and follow us @ForgeRock