ForgeRock

DATASHEET

ForgeRock User-Managed Access (UMA)

Secure Delegated Authorization that Cultivates Privacy, Consent and Trusted Relationships

Privacy regulations, such as the General Data Protection law (GDPR), or the California Consumer Privacy Act (CCPA), or Australia's Consumer Data Right (CDR), impact all organizations holding or processing personally identifiable information (PII). Organizations can suffer disastrous repercussions in the form of enormous fines and even imprisonment of executives if they fail to comply. Further, lax privacy practices can cost an organization reputation and ultimately consumer trust. But privacy regulations don't have to impede business. Savvy organizations leverage these regulations as a way to build trust with their customers. They opt for a contextual privacy methodology that puts more choice and control into the hands of the consumer — ultimately building the trusted relationships necessary for successful digital transformation.

ForgeRock User-Managed Access is a privacy and consent solution based on UMA 2.0 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 can delegate data access to others through a simple "Share" button in your apps, and can monitor and manage sharing preferences through a central console. Organizations can build customer trust, overcome privacy and consent challenges, and create new revenue opportunities.

What is UMA?

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, CCPA, 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 IoT benefits.

Highlights

- Consumers can grant, monitor, deny, approve and revoke digital consent.
- Consent can be granted ahead of time ("Share") and approve access after it is requested.
- Consumers manage sharing settings for multiple data sources from a single centralized console.
- Organizations can easily add delegation capabilities to entire partner app ecosystems without the central authorization server seeing any of the partner data sources.
- Authorization decisions are as fine-grained as the protected APIs' scopes.

Features and 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 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.

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.

"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

PHILIPS

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 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
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.

UMA 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.

Learn More About How UMA Can Help Your Organization

With full support for UMA, ForgeRock helps organizations build customer trust and unlock new opportunities. **Contact us** or visit **ForgeRock.com** to learn more.