Privacy by Design Implications of UMA

Privacy by Design Implications of UMA

It is useful to examine how User-Managed Access (UMA) relates to the seven foundational principles of Privacy by Design (PbD). This document provides an analysis of each principle and how UMA and UMA-enabled solutions can support the principle. Since PbD was developed, the EU General Data Protection Regulation (GDPR) incorporated the notion of "Data protection by design and by default" in its Article 25. This document also includes a similar analysis of the GDPR construct.

The UMA Legal effort is working to provide an operational solution for accelerating the adoption, deployment, and use of UMA-enabled services in a manner consistent with protecting privacy rights.

Privacy by Design Principles and Analysis

Proactive not Reactive; Preventative not Remedial

This principle is key for promoting meaningful, informed, uncoerced consent, and most especially for interactive consent experiences that are more empowering than a traditional opt-in choice at when an online service user is forced to make a service usage decision. Allowing an individual to choose a data sharing option well before – or well after – a tempting offer is on the table enables full consideration.

In healthcare, efforts to ensure patient right of access and patient-directed data sharing exemplify part of this principle.

While many systems focus solely on gathering user consent at the time of the access request, UMA enables users (human beings in the "resource owner" role of the UMA protocol) to choose access policies before a data requester attempts access. It also enables resource owners to to consider data access requests and approve or deny them, either right away or at some time of their own choosing. This enables a different relationship between resource owners and requesters. As noted in a W3C privacy workshop position paper focusing on UMA, "Granting access to data is then no longer a matter of mere passive consent to terms of use. Rather, it becomes a valuable *offer* of access on user-specified terms, more fully empowering ordinary web users to act as peers in a network that enables selective sharing."

Privacy as the Default Setting

This principle captures the importance of user actions that follow the path of least resistance so that the user experience design is human-centered. As noted by Don Norman in *The Design of Everyday Things*, "Everyday activities must usually be done relatively quickly, often simultaneously with other activities. .... Much human behavior is done subconsciously, without conscious awareness and not available to inspection. .... Subconscious thought is biased toward regularity and structure, and it is limited in formal power. It may not be capable of symbolic manipulation, of careful reasoning through a sequence of steps. [2002 ed., p. 125]"

UMA enables an authorization server (a service in the UMA role of managing a resource owner's access policy settings) to offer a variety of data sharing controls to users, centralizing these controls so that access blocking can easily be applied across any number of resource servers (services in the role of data hosting). A "default-deny" (block sharing by default) approach is expected and discussed in the UMA standard, and profiles such as Health Relationship Trust (HEART) are being produced in order to tighten controls even further.

Privacy Embedded into Design

Embedding high-quality privacy controls into online service development is a goal not often achieved – except in services designed specifically to address consumer privacy concerns. (The advent of the GDPR and other similar regulations with global impact will likely have some effect.)

UMA, of course, exists to enable a resource owner – the "user" in User-Managed Access -- to control the authorization of data sharing and other protected-resource access made between online services on his or her behalf, or with his or her authorization by an autonomous requesting party. Any online service that leverages UMA as its resource protection mechanism is enabling a whole new level of embedded privacy controls, using an open protocol that is designed to be as friendly to developers as possible to facilitate adoption and interoperability. UMA's first design principle is "Simple to understand, implement in an interoperable fashion, and deploy on an Internet-wide scale."

Full Functionality - Positive-Sum, not Zero-Sum

This principle is important for including all parties affected in the conversation. Often, user empowerment equates to service disempowerment, and this is why we see little uptake of some privacy enhancement technologies.

UMA strives to offer benefits to all of the actors in a digital service ecosystem. For example, making use of a combination of policy definitions and the ability of an authorization server to gather "claims" from requesting parties who wish to access data, a resource owner define who is in her "family circle" exactly once, then reuse that definition across sites to control sharing of the data she manages in all those places. And a data-hosting or Internet of Things service (resource server) can benefit from outsourcing user data access control to a centralized authorization hub for the same reasons that it might outsource user login to a social sign-in identity provider: to concentrate on what it does best, leverage a third-party service's special expertise and knowledge, and get more functionality with less effort. Where authentication has seen innovation through standards-based social sign-in, authorization for the purpose of privacy could see innovation through standards-based "social access control".

The UMA Legal effort, in combination with Kantara trust frameworks, could ultimately help set rules for all the parties participating in an "access federation" that involves loosely coupled UMA services, apps, and individuals.

End-to-End Security - Full Lifecycle Protection

Privacy has a synergistic relationship with security and other system controls. This principle recognizes the important role of comprehensive protection.

UMA applies security protection at the interfaces of each of its interacting entities: resource owner, authorization server, resource server, client, and requesting party. resource owner and requesting party. Most of its protections come from its OAuth and TLS technology basis. Additional protections can be applied through business and legal processes, auditing of protocol artifacts, and likely the suitable application of Consent Receipts and additional "receipt"-style artifacts. (The resource server itself is responsible for all required back-end security defenses that protect the resources at rest.)

Visibility and Transparency - Keep it Open

Proprietary access control mechanisms used by digital services do nothing to aid this principle, and often give cover for improper sharing. At the same time, service operators struggle to find cost-effective ways to increase user visibility of data sharing.

The UMA Legal effort is designed to map proper behavior by all UMA parties to their protocol-level actions, and ultimately make them auditable for non-repudiation. This mechanism strives to maximize enforceability of behavior norms, given that data sharing typically has few other practical mechanisms available for restricting downstream data usage. This provides the underpinnings for higher-order agreements, assessment, accreditation, enforcement, and liability mechanisms.

Respect for User Privacy - Keep it User-Centric

This principle captures an admirable aspiration. A key challenge in meeting it comes when digital services serve *users* that are not themselves service *cust omers*; as has often been noted, they are instead the *product*. This sets up conflicting and even perverse incentives. Thus the irony of Facebook – with its particular business model – being pressured to have a user-centric privacy policy.

The draft UMA Legal business model document (forthcoming) exists to make the case that (emphasis added) "UMA can provide the *autonomy, reciprocity, and objectivity* to grow market trust in widely sharing access to personal digital assets with devices, apps, and internet databases."

GDPR Article 25 (Data Protection by Design and by Default) and Analysis

Much more could be said about UMA's impact on the GDPR and its intent (for example, Article 7, "Conditions for consent", and related Recitals). However, this analysis focuses solely on Article 25.

P1: Implementing Data-Protection Principles

Paragraph 1 is broadly about the data controller implementing technical and organisational measures (such as pseudonymisation) to achieve data-protection principles (such as data minimisation) to protect data subject rights.

Looking at the technical level, UMA (like its substrate, OAuth) is *about* authorization, and *relies on* identity and authentication. This means it largely inherits the properties of whatever identity, authentication, and federated authentication systems are used to implement it. Either local or federated authentication can be used with UMA. Pseudonymisation of the resource owner can be preserved between the resource server and authorization server. OAuth (or OpenID Connect) is used to connect them; if the latter is used, an identity may be shared. The authorization server becomes aware of requesting party claims based on the resource owner's requirements for policy conditions to be satisfied. See the privacy considerations in the two UMA specifications.

Looking at organisational (business and legal) levels, this is where the UMA Legal effort, trust frameworks, and service assessment criteria may have a role to play.

Ensuring Only Necessary Personal Data Are Processed

Paragraph 2 is broadly about ensuring only necessary personal data are processed, taking into account the amount collected, the extent of processing, the storage period, and access controls.

UMA has an authorization server component (familiar from OAuth but able to be broken out from its companion resource server component through UMA standardization). This service is unique in that it is not a data controller interacting with the individual in a typical sense, nor is it a data processor. Rather, it is an agent for the individual, able to act on their behalf in determining where personal data flows without holding any of that data. UMA ensures that data does not have to be aggregated by a central service in order to be protected.

The process of claims-gathering and the UMA Legal effort can enable "resource owner-directed sharing terms and conditions" to apply to requesting parties and clients, thus imposing business- and legal-level constraints on the extent of processing and the storage period.

Becoming Certified

Paragraph 3 is about enabling organisations to demonstrate compliance with the GDPR through an approved certification mechanism.

The appropriate UMA parties could ultimately make use of the UMA Legal effort, and possibly one or more Kantara (and/or other) service assessment criteria accreditation frameworks, for certification.