XDI Link Contracts: Building Blocks for Privacy-Protecting Trust Frameworks

[insert author names here]—OASIS XDI Technical Committee

About XDI

XDI is a structured data sharing protocol under development by the OASIS XDI Technical Committee [1] for describing and sharing data using XRI-addressable RDF graphs. The main features of XDI are:

- The ability to link and nest RDF graphs to provide context;
- Full addressability of all graph nodes at any level of context;
- Representation of XDI operations as graph statements so portable authorization can be built into the graph (a feature called XDI *link contracts*);
- A compact JSON serialization format in addition to XML;
- A simple ontology language for defining shared semantics using XDI dictionary services.

XDI link contracts are particularly relevant to Internet authorization protocols such as OAuth [2] and User-Managed Access (UMA) [3]. These protocols specify how to obtain and use tokens to access a protected resource, but do not establish shared semantics about the data being exchanged or permissions being granted. XDI link contracts fill that gap.

About Personal Data Stores (PDS)

PDS is a concept arising from the field of Vendor Relationship Management (VRM). To quote from the ProjectVRM home page at the Harvard Berkman Center [4]:

> *VRM stands for Vendor Relationship Management, a term that was coined as a customer-side counterpart for Customer Relationship Management, or CRM — a multi-billion-dollar worldwide industry that provides companies with tools to manage their relationships with customers.*

VRM is based on the premise that individuals can have the customer-side equivalent of a CRM system. This repository has come to be known as a *personal data store* (PDS). There is no requirement for a PDS to be centralized; in fact the preferred design is for it to be virtual control point for the data a person may have stored at many different locations on the net (e.g., financial records at a bank; medical records at a hospital; academic records at a school, etc.) An individual can then exert control over the sharing of this data via one or more *PDS endpoints* that speak protocols like OAuth, UMA, and XDI.

About Trust Frameworks

The following definition is from the Open Identity Exchange [5], an international non-profit organization established in March 2010 to serve as an industry-neutral trust framework platform:

> *In the context of digital identity systems, a trust framework is a certification program that enables the party who accepts a digital identity credential (called the* relying party*) to trust the identity, security, and privacy policies of the party who issues the credential (called the* identity service provider*).*

In essence, trust frameworks provide a way to bind the technological "tools" for exchange of digital identity data to the policy "rules" governing the parties to this exchange. The result is a powerful new tool for the adoption and enforcement of data security and protection policies among Internet-scale communities. For example, the first operational OIX trust framework, the U.S. ICAM Trust Framework [6], applies to the entire United States public when visiting a U.S. federal website.

Using XDI Link Contracts for Privacy-Protecting Trust Frameworks

The combination of XDI, PDS, and trust frameworks can be the basis for a new approach to Internet-scale privacy management. The essential elements of this approach are:

1. Individuals begin establishing PDS services (with one or more PDS service providers) to make their personal data a protectable resource on the Internet.
2. PDS service providers, governments, vendors, privacy advocacy groups, and other stakeholders begin defining trust frameworks that specify the privacy requirements for handling of PDS data.
3. Vendors begin accepting PDS data shared via XDI link contracts that bind the sharing of this data to the privacy controls specified by these trust frameworks.

This is a win/win/win approach:

1. Individuals win because their personal data can now be shared and tracked in a manner over which they can exert direct control.
2. Vendors win because they can receive fresh, highly relevant personal data under a self-reinforcing mutual trust relationship.
3. Regulators and PDS service providers win because they can let market forces establish the trust frameworks under which both individuals and vendors will choose to participate.

References

[1] OASIS XDI Technical Committee, http://www.oasis-open.org/committees/xdi/
[2] OAuth, http://oauth.net/, and OAuth 2.0, http://oauth.net/2/
[3] User Managed Access (UMA),
[4] Project VRM , http://blogs.law.harvard.edu/vrm/about/
[5] Open Identity Exchange, http://www.openidentityexchange.org/
[6] US ICAM Trust Framework, http://openidentityexchange.org/trust-frameworks/us-icam