Personal Digital Identity Management
The Sxip Network Overview

Version 1.0

Dick Hardt
July 22, 2004

Abstract

The problem of finding the best way to safely store and share the identity data that distinguishes one user from another on the web has hounded both companies and individuals for years. Most websites use a stand-alone authentication system, so users struggle to manage multiple accounts, while sites lose customers due to lengthy log-in processes and forgotten passwords. Online operators are desperate for ways to share and update user information, check to see if users have authenticated reliably, and offer authorizations for system access. They want to do all of this while still protecting the privacy of their users and limiting their own liability.

The Sxip Network, a cooperative public identity network running an open protocol, grew from efforts to build a balanced solution that meets the requirements of the entire community. In order for a user to maintain a persistent identity across the web, there must exist a central authority mapping globally unique identities to sites that are authoritative for them – just like the central DNS the Internet relies on. Beyond that, a great deal more centralized control is undesirable. In recognizing these two factors, the Sxip Network is architecturally different from existing identity management protocols, the same way the Internet itself is different from the private networks it has come to replace.

Contents

Introduction

How the Sxip Network Operates

The Sxip Network started with the premise that web users should be able to associate certain personal data properties of their choosing under one or more "personas". For example, a web user might wish to maintain a separate persona for work, entertainment purposes, and school, and also to remain anonymous when convenient. The Sxip Network associates each of a user's personas with 64 bit value called a GUPI, or Globally Unique Persona Identifier, which remains persistent across the web. Properties are only exchanged when a user is present to give real-time permission, and they are only exchanged over the web. When a participating website, or "Membersite", wishes to authenticate a user or query for a user's properties, the Membersite sends a message to the user's Homesite using the Simple eXtensible Identity Protocol, or SXIP.

How the Data Moves

Data exchange between Homesites and Membersites happens through a seamless process that transmits either simple name-value pairs or richer XML properties through a series of browser posts. When a registered user visits a participating Membersite, his or her browser is redirected to a sxip.net shadow domain at the Membersite which allows it to get a cookie indicating the Homesite where the visitor is likely to have an account.

SXIP allows for an ever-growing list of properties to be associated with GUPIs and transmitted to Membersites of the web user's choice. It is anticipated that as the protocol evolves, the Sxip Network will be put to use for more than just easier registration and faster logins. Ultimately, the Network allows website visitors to prove they have certain properties, such as group membership or student status – true digital identity.

Sxip Network Philosophy

Minimal New Trust Required

The Sxip Network relies on existing trust relationships. To begin, all participants start with the trust that a Rootsite's authority mapping GUPIs to Homesites has not been compromised.

The user is in charge of directing which data gets posted from the Homesite to the Membersite browser page, so the Membersite need only trust the user and the Homesite's authentication mechanism.

Simple to Deploy

Implementing Sxip is easy. Our open source SDKs are downloadable for a variety of different languages. Adding to existing websites can be done in a couple of hours using tools such as our Simple Site Server and our Account Linker. Alternatively, you can tailor the Sxip solution to meet your unique requirements using our well-defined protocol and schema. Demos and specifications are provided for training purposes.

Site Determines User Experience

The Sxip Network is a platform, not a product. Design requirements are kept to a minimum and used only to ensure a consistent experience for users. Sites are not obligated to follow implementation guidelines. Participating websites are free to innovate on how to create a user experience suitable for their customers.

Data Interchange Facilitated

The Sxip Network makes it easy for sites to keep user information current. With the Sxip Network, Membersites are able to easily ask for new user properties with every session without needlessly inconveniencing the user. The user can select to be prompted for the release of any property, only prompted for updated properties, or not prompted at all.

Extensible

The Sxip property list is extensible, enabling sites that want to create new applications to do so easily. Using XML for rich properties can extend the types of properties that can be stored and retrieved. The Sxip Network's goal is not to make new schemas but to leverage existing schemas, which will be used whenever possible. Changing or extending the schema for the properties list is an open and regular process. Approvals will be handled by the community.

Distributed Architecture

The Sxip Network is loosely coupled, a hierarchical distributed architecture. With only the DNS and GUPI mappings stored at a Rootsite, the rest of the data and all the user data communications are done by sites belonging to the Sxip Network though not visible to Sxip, providing a very scalable system.

Open and Accessible

The Sxip Network was designed to offer choices to the online community. Implementations for all popular application platforms are or will be available. The protocol is not dependent on any browser. Any site can be a Membersite, and any site can be a Homesite.