HP Vision for Federated Identity Preferences and Policies (FIPPs)

Author: Joe Pato (HPL) joe_pato@hp.com
Contributors: Marco Casassa Mont (HPL), Owen Rees (HPL)

20 January 2002

We envision identity, preference and policy systems that will enable entities to interact electronically in personal, social and work contexts as fluidly as individuals do in inter-personal relationships. Participants will be confident in the control of their reputation. People will remain comfortable in how their personal information is handled while organizations gain value in the quality of information they are receiving and mechanisms for specifying and enforcing policy controls.

We explain here the goals of identity, preference and policy systems by considering the potential experience of a traveling sales representative who is taking advantage of such a system. We then consider some underlying principles for these systems and some of the critical components that play a role in the environment.

Vision

Day-in-the-Life Scenario

Ginger Smith, a sales representative for ACME pharmaceuticals, will be visiting a potential new customer, Mega-Health Cooperative, today. To be sure to be on time for the early morning meeting, Ginger has spent the night at a conveniently located hotel.

Upon waking, Ginger activates her PDA giving it a voice command to display breaking news relevant to Mega-Health. The information, displayed in the hotel's in-room TV, is gathered from a variety of industry clipping services subscribed to by ACME, with content selected by Ginger's preferences. In one corner a story is outlining changes to HIPPA privacy regulations. The source is a pay-per-access subscription service, so Ginger issues another voice command to pay the fee and display the details. Ginger's PDA uses speaker verification techniques to authenticate Ginger and then proceeds to initiate the request for content and the corresponding

payment from the ACME account. Satisfied that the information will contribute to the sales pitch, Ginger checks out of the hotel by instructing her PDA. Again, charges for the stay are posted to the ACME account, but the charge for in-room movie rental and the terry-cloth robe to take home are posted to Ginger's personal credit account.

This is Ginger's first visit to Mega-Health, so upon arrival she checks in with the security desk at the front gate. Her visit is expected, but as she will be entering a restricted area, the security guards want verification that Ginger is in fact a legitimate sales representative for ACME. Ginger presents her PDA, which is now displaying her virtual business card asserting her role as a regional sales representative for ACME. While presenting the display, Ginger activates the finger imaging unit on the PDA which causes an identity confirmation display and transmits an electronic credential to the Mega-Health security desk. As part of the mechanism for transmitting the credential, ACME's security policy service verifies that Mega-Health is a potential customer and that Ginger is authorized to represent ACME today. Mega-Health verifies that the credential was issued by ACME and in turn issues a new credential certifying that Ginger has access to public resources within the Mega-Health site. As in all transactions that require one of Ginger's identities, her PDA records information about the persona that Ginger has presented to Mega-Health as well as the privacy policy that Mega-Health is publishing.

Initial conversations with Mega-Health go extremely well, so Ginger decides to provide additional clinical trial data to close the deal. To present this effectively, she chooses to display a spreadsheet from the corporate data store and establish a video link to the lead investigator for the trial. The credentials she obtained from Mega-Health that morning enable Ginger to access the Mega-Health network with her PDA. ACME credentials allow her to create a virtual private network to the ACME corporate network and to find and connect to the lead researcher.

Mega-Health is impressed. The deal is concluded when Ginger and the procurement officer for Mega-Health digitally sign an order.

Observation

While some of what our scenario portrays is beyond the environment that identity and preference services are pursuing today, many of the elements described are currently practical and will certainly be feasible within a few years. We explore this combination of emerging capabilities with slightly over the horizon directions to develop a longer-term vision that will guide development and policy with stability over several years.

Key Attributes

1. Personal control

We seek to improve the electronically mediated experience for people. Therefore, we believe that the system must be responsive to the desires and concerns of individuals and that users must have the ability to determine how they interact with the systems rather than having these systems impose a singular view.

2. Privacy

Participants must be justifiably confident that their privacy is being protected.

3. Simplicity

The system must be easy to understand, easy to deploy and easy to administer.

4. Ubiquity

Over time, the system must be available to everyone for all kinds of interactions – from web services, to peer-to-peer communication, from personal devices to shared utility kiosks.

5. Heterogeneity

Universal availability implies heterogeneity. We must provide systems that transcend hardware and software alignments – that keep the value delivered to end-users and relying parties as the motivational driver.

Characteristics and Requirements

1. Personalized experience

The essence of an identity, preference and policy system is to customize the interactions individuals experience when dealing with services. This customization applies at the discretion of the individual for all services with which they interact with rather than each service presenting a distinct model.

In the scenario personalization occurs in many areas. One example is when Ginger's PDA retained information about every system that requested Ginger's identity.

2. Freedom of choice

We expect that freedom of choice will apply to the kind of providers that supply identity, preference and policy services, to the kinds of hardware that provides the electronic interaction and to the kinds of mechanisms that perform authentication.

Freedom of choice is implicit in the scenario. Mega-Health and ACME use different credential issuing authorities, Ginger uses her own PDA rather than a device issued by ACME.

3. Federation

Information about an individual and even the identities (or personas) assumed by that individual may be different in different contexts. A federated identity, preference and policy system acknowledges this flexibility and also recognizes that multiple parties may hold the information. Federation provides the model and mechanisms for constructing the aggregate view of the individual in a fashion that is controlled by the individual.

Federation occurs in a variety of situations in the scenario. Some examples include: when preferences are obtained for information feeds, when identity credentials are maintained for information services, ACME employee verification and access to Mega-Health public resources.

4. Automation

The electronic world lacks the physical cues present in real-world interactions. Therefore, identity and preference systems must provide automated assistance in making trust decisions.

In the scenario, automation enables the selection of the proper payment context as well as the trigger to involve ACME security policy when presenting a credential to Mega-Health.

5. Incremental Evolution

We expect that the capabilities of a federated identity, preference and policy system will emerge incrementally. A system must accommodate this evolution and provide mechanisms to evaluate the relative maturity of components of the system.

In the scenario we assume biometric authentication techniques embedded in the client device. In many cases, it will be sufficient to deploy simpler password or even PIN based authentication of the end-user to the client device.

System Actors & Components

Identity, preferences and policies are the quantities that the system will manage for us and make available to the following actors:

End User

The end user is the individual accessing services through some set of clients. The end user is the entity about whom preferences are stored and identities are asserted.

In our scenario, Ginger Smith is the end-user.

Client

Clients are responsible for the user-experience, orchestrating interactions with other parties. The client is responsible for authenticating the end-user and maintaining a close association between the point of access device and the end user. The client projects the end-user's electronic identity and preferences to relying parties in a fashion controlled directly by interaction with the end-user or as determined by preferences established for that user.

A client can either be a single self-contained device, or it can be a collection of components, including proxies, that fulfill the role described above. Similarly, the client may retain preference information locally in a repository or retrieve user preferences stored at a service.

Throughout the scenario, the client appears to be Ginger's PDA. However, when Ginger is gaining access to the Mega-Health facility, the client expands to include the policy services resident at ACME's security service. In this way we see that the client is not simply defined by the point of access device, but by the collection of systems that orchestrate the interactions for the end-user.

Relying Party

The relying party will consume information provided by the client. The relying party is any entity, though frequently a service provider, that is dependent on the truthfulness of the data presented by the client. The relying party may require an authority to validate the information provided by the client.

The relying party may construct a local profile for the user (presuming compliance with data privacy regulations), but should be constructed to accept the presentation of credentials and reputation information from the client. It is likely that the relying party will always augment the profile information that is disclosed by the client with observations of transactions with the given relying party. This information can even impute certain reputation to the client by having correlated behavior with other data.

The relying party may use a repository for its policy information.

There are many relying parties in the scenario. They include: the hotel, the premium information provider, the Mega-Health security checkpoint, the ACME credential introduction service, the ACME information repository, the ACME video conferencing

service, the Mega-Health network. In each case, the relying party examines information provided by a client and determines if and how to satisfy the client's request.

Issuing Authority

The issuing authority is responsible for establishing the quality of the information – it is responsible for certifying identity and other attributes to some level of quality as determined by the operating rules.

ACME is the issuing authority for Ginger's employee credentials. Mega-Health is the issuing authority for credentials to access the Mega-Health facility and public resources. A number of other unidentified authorities issue credentials for Ginger to access information services and complete payment transactions.

Repository

The repository contains user preference or organizational policy information. The repository can either be closely held, or be a service. If it is a service, the data may be visible to the operator, or it may remain private (encrypted) – further, if it is a service, the service may be provided by a collection of providers no one of which has direct visibility into the information being stored.

Ginger's PDA is the repository for her personal preferences; ACME and Mega-Health maintain repositories for their corresponding security services.