

2215 passes shipping information and payment settlement information to service provider **2205**. Service provider **2205** then passes payment (e.g., billing) information **2230** to its preferred payment provider **2235** for processing.

[0170] FIG. 23 is an interaction flowchart illustrating a token-based wallet service. When service providers contact other service providers for services such as credit card processing, transient tokens such as one-time credit card numbers can be issued and then resolved by only the service provider (e.g., a payment provider) that actually uses the information. Transient tokens have the property of being an opaque, random or pseudo-random nonce. The property of being a nonce is a countermeasure used to deter replay attacks. Randomness in such a token protects the token from being guessed by an adversary.

[0171] In the illustrated example, a transaction at a service provider merchant occurs without the service provider merchant learning the user's address or credit card number and only receiving transient tokens or pointers for each. Service provider **2305** requests payment **2310** from identity provider **2315**. Identity provider **2315** authenticates the user and authorizes the requested transaction **2320**. Identity provider **2315** then generates and passes a payment token **2325** to service provider **2305**. Service provider **2305** sends the payment token **2330** to payment provider **2335**. Payment provider **2335** can then use the token to request payment information **2340** from identity provider **2315**. In response to this request, identity provider **2315** sends the actual payment information **2345** (e.g., credit card number) to payment provider **2335**. One skilled in the art will recognize that in other embodiments additional service providers, for example, a shipping carrier could similarly use transient tokens or service tickets to interface with identity provider **2315**.

[0172] 6. Security

[0173] In an embodiment, web service requests are secured by public-key infrastructure (PKI) encryption with public-key certificates on both sides of the connection. In one embodiment, certification authorities can add a distributed network identity element to the certificate's distinguished name to certify the public-key certificates. In an alternate embodiment, a certificate policy is used rather than amending the certificate's distinguished name. A certificate policy is a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. Further, web service calls include an assertion in their header that can be verified in the user profile data stored by the identity provider. As described above, one skilled in the art will appreciate that SAML assertions are an example of an assertion language that can be placed in SOAP envelopes.

[0174] 7. User Profile Services

[0175] Policies are used to define user-specific privacy rules that control how an identity provider disseminates user profile data and preferences to service providers or other identity providers. In an embodiment, an identity provider provides a profile service for the user in which different sets of user preferences (or attributes) are grouped with associated policies for privacy. For example, the user could have attributes such as "address" and "phone number" with an associated policy statement that these cannot be released to

service providers without the user's express acknowledgement. Additionally, the user could have "favorite restaurants" and "location" attributes that can be shared with service providers without an acknowledgement. Users can further set policies for classes of services, such as weather reports and restaurant searches, that permits these service classes to request user profile data without authentication. Table 5 includes example user policies, however, one skilled in the art will recognize that numerous additional policies can be implemented.

TABLE 5

Example User Policies	
Policy	Description
Public Acknowledgement Required Contract	Anyone can access the information Requires user's confirmation every time Can be released to service providers that user has identified
Anonymous	Service provider can only get pointer or handle to the information

[0176] In another embodiment, a user can specify the manner in which a service provider handles user profile data and preferences. For example, the user can select whether (1) the information is to be used only once and discarded, (2) the information can be saved and reused, (3) the information can be forwarded to another service provider only once then discarded, or (4) the information can be forwarded to other service providers with restriction. The identity provider provides these features for the user, either for individual attributes or on a group of attributes (e.g., a specific profile). Further, users can customize these data control for each service provider in the identity provider's user directory.

[0177] FIG. 24 is an interaction flowchart illustrating user policy validation. In an embodiment, when a service provider requests information about a user from an identity provider, the identity provider validates the request against user policy and preference settings. According to one embodiment, service providers include the following in a request: (1) handle for the user, (2) list of user attributes requested, (3) privileges required for each attribute, and (4) whether the attribute's true value or handle is required.

[0178] In the illustrated validation flowchart, service provider **2405** requests user data **2410** from identity provider **2415**. Identity provider **2415** optionally validates the user's credentials and the signature of service provider **2405** (not shown). Next, identity provider **2415** determines whether the data request can be approved **2420** consistent with user policy and preferences. If the user's general service provider policy or service provider-specific policy is consistent with the data requested, then service provider **2405** receives user data (or pointer) **2425**. In the case where the data requested is not consistent with the general or the specific user policy for service provider **2405**, identity provider **2415** requests user validation **2430**. In this manner, the user has an opportunity to view the data request and the policy conflict and to accept or to reject the release of the information. If the user decides to make a policy exception **2435**, then service provider **2405** receives the user data **2440**.