THE INFORMATION TRUST EXCHANGE

http://www.infotrust.org

Trust, identity, personalization,
content and user sharing for the news industry

CONCEPT PROPOSAL
USER AUTHENTICATION/DATA-EXCHANGE SERVICE

(Drafted by Scott Bradner/Bill Densmore)

PREMISE:

A core service to be offered by ITEGA, or private entities licensed by ITEGA, is a "federated authentication" service that supports not only single sign-on, but also the permitted transfer of key user attributes among the independent services that use the ITEGA services. Think of it as open Facebook Connect login governed by a public-benefit nonprofit. Many things fall out of this core operation -- sharing of identity and preference info, subscription info and payment notation, personalization of content (and advertising) if compliant with EU rules and as permitted by the users. Importantly, there can be a plurality of "registrars" of users. Another analogy is to the academic EduRoam service that allows faculty at U.S. universities to log into wifi at all other participating campuses.

BASIC SERVICE

1. Authentication - providing a service that authenticates a web user as a subscriber to one or more ITEGA-compliant services.

2. Verifying group membership -- being able to assert that a particular web user has subscribed to a particular group of services (e.g., access to a specific set of publishers). A publisher will be able to verify that the web user has paid for access to a group that includes that publisher's content (or portions of the publisher's content).

Note that the above do not, by themselves provide any identifier for the user. The users will be able to subscribe to different levels of service in addition to different service groups.

- Level 1: The most expensive service level is one in which the publisher is not provided any user identifier, just an assertion that the web user has been authenticated and has paid for access to that publisher's content.

- Level 2: The publisher is provided a unique identifier for the user but that unique identifier is also unique to the particular publisher. The publisher can set up their own database to track that user's activities on their own site. The publisher can also ask the user for additional information (e.g., name for personalization) and add that to their database.

- Level 3: The publisher is provided a unique identifier for the web user but this identifier is not unique to the specific publisher -- the same identifier is provided to all publishers the web user accesses. The publishers can use a third party to track the user activities across publishers.

- Level 4: The publisher is provided with the web user's name and email address, and possible other permissioned attributes.

WHAT IS RECORDED?

The authentication service need not have any permanent database of user logins or activity; the authentication token can "time out" and be deleted after a period.

Access by a user to resources does not have to be logged or saved unless there is some reason to do billing on an individual-event basis. While the service might want to be designed to include the addition of a "logging service" for such purpose, **we are tentatively concluding it should be outside the scope of ITEGA to facilitate this, as it will raise important privacy questions if implemented.**

WHAT NEEDS TO BE BUILT?

Scott Bradner believes the Shibboleth open-source authentication service, used by major universities and other organizations, can form the basis of ITEGA-supported technology to perform the concept authentication and data-sharing services listed above. He has years of experience managing such services and participating in related standards bodies. No hardware would be purchased, the service would run on one or more cloud services and would therefore be abundantly scalable.

The other component will be software that has to run on publishers' servers. Support for the different levels of service described above is standard in Shibboleth environments and is available as open source.

The two key premises this approach implies are: (1) Minimize information in the central user database, to comply with GDPR and (2) The authentication service itself doesn't keep any demographic or interest information.

WHAT WILL IT COST?

Scott believes there are developer resources in the Boston area who can build these services reliably in the price range of $150K to $200K FTE per person in a matter of months, not years. He estimates 3-4 people would be an optimum development team. Based on this, an estimate of resources required might range between $500K and $1M. Our three-year concept budget only proposes $280K in first-year development; this was on the assumption that private vendors would undertake major develop work on the basis of future ITEGA-network revenue opportunity. **This may need to be thrashed out a bit more as a premise.**