Notes from Identity Breakout session (11:15-Noon, Nov 2, 2011, room: California 2)

Mahalingam Mani

Background:

Webrtc wg which met mon&tue. continually dealt with security considerations related to JS application trust model, origin policy, one-time vs. long-term trusted access for application websites, callers and callees being a few.
Among them what appeared to be core to establishing any trust model for end-end assurance that the caller and callee have on each other's identity.The upshot, in my personal summary, was to arrive at a user identifier type that can be used to ubiquitously, unambiguously and seurely establish a session and engage in two-way communications with due identity-protection and privacy safeguards in the process of doing so; without assuming any form of trust of the service providers, viz., signaling and media intermediaries.
Openid for federated authentication on the Internet; Oauth mechanism for federated delegated authorization; and even some manifestation of browserid mechanism from Mozilla were discussed.
The primary distinction for the classic federated authentication model of client-AP(Asserting Party aka Identity Provider)-RP (Relying Party) model seems to me to be that in the case of webrtc model; the RP is not the usual SP but the remote client (caller and/or callee). In fact we don't trust the SP with content and control (though SP itself may be interested in the clients for its accounting and other purposes of accountability)

It appears that the email-Id is the most obvious and ubiquitous identifier for federated communications across multiple identity providers. Communication within an administrative domain itself may degenerate to reference to handles (and other resolvable aliases within the domain). Both models are not themselves new and are already the de facto identifiers in most contexts. So what is the issue if this is such a no-brainer?
Summary:

The webrtc intersects many other communication protocols (SIP, XMPP, PSTN,...) and translating identifiers and formats (SIP URI and XMPP addresses) is another consideration; also it finally boils down to the realm-namespace tuple for unique universal identification as in contactbooks and directories; as also about need to have a web-of-trust between the realms in communication. DNS-based Domain-names offer the basic naming framework for realms (each governed by its autonomous security policies).

The other challenge is whether this can be done without requiring explicit consent every time - that leads to how one qualifies long-term accesses to websites; and to users.
Some generalized Manifestation of browserid appears to offer some possibility
But appears fraught with revocation-related risks.

CSP CORS considerations (being enhanced in webappsec wg) and client-security considerations of federated social-web seem to have considerable overlap with this. So is work related to (device and user) permissions and policies in DAP combined with identifiers in contact APIs.
Thus - the overlapping work is worth coordinating to avoid duplicate definitions, APIs; as part of already Evolving joint task forces in other areas.