Google Doc: ite-single-sign-on-network-description-v2-02-22-19

Infotrust
eXchange

**Information Trust Exchange Governing Association**
**http://www.itega.org**
https://docs.google.com/document/d/19bL2TrSKBjO3ymSDIaUxCWo_efmwMLJEQVCq3aXGrlI/edit

# A discussion of a Single Sign On network authentication service featuring unique, network, anonymized common IDs

By Richard Lerner and Bill Densmore
(terminology: http://newshare.com/ite-demo/it-architectdure-DIAGRAM-V2-01-17-17.pdf)

22 Feb 2019 -- Revised for public viewing
17 Jan 2017 - updated for ITEGA
7 May 2012 - initial version

## Implementing a federated-authentication, single-sign on (SSO) service for ITEGA prototyping

### Overview

The ITEGA-Network allows customers from multiple sites to authenticate on all sites within the network, using the account on their home site. Only the home Site (Identity Service Provider, or IdSP) ever receives or authenticates a customer's username and password. Functionally, each member site can collect and store personalization information for remote accounts, as may be required by the site, as may be permitted by law or ITEGA network governance. The personalization information can come from any of three sources:

1. Directly from the customer via a forms submitted to the customer’s IdSP (as data controller) and then shared across the ITEGA-Network in conformance with use consent provided by the customer. This is first-party data.

2. Copied from common data sent from the home server and shared via the ITEGA-Network server according to use governance under the real-time control of the customer.

3. Copied from the Customer Profile Network (the Data Demographic Aggregator, DDA, or anonymous User Data Exchange) server. The DDA only has information supplied via the customer's home IdSP and only linked to an anonymous key (explained more fully below).

The latter two allow the customer to provide information that follows them around the network. If the DDA can distinguish between network clients and third-party clients, it may be possible to forego #2, above, and have all personalization information pass through the DDA / Customer Profile Network. Otherwise, we need to define a common set of demographics to pass through the ITEGA-Network server.

If the DDA is constantly updated by the IdSP whenever sharable profile information is changed by the customer at her IdSP, then there is no need for the NTEGA Network Auth-Logging Service to have any dynamic data on the user. But there may be some very basic information about a user (such as their globally unique anonymous user ID) that needs to be available real time universally to address billing and login issues, but not demographic issues. That should probably be part of what is authenticated -- and then stored on a session-basis by the auth/logging service.

The particular DDA where with the IdSP is affiliated -- and there may be at scale a plurality of DDAs for different topical/geographic/use networks -- can hold the detailed demographic data but on one side -- the side which works with IdSP's, it is specific to a unique user ID. On the other side -- the side which deals with Profile Usage Agents (advertisers and nonpublishers) it is anonymized.

## ANONYMOUS SESSION NETWORK ID

The home server (hIdSP) maintains a mapping from its internal userIds to networkUserIds assigned uniquely for each remote server the customer authenticates with. So, if a customer is registered on HOME with userId 12345, and she attempts to authenticate on REMOTE-1, HOME her profile will assign a new networkUserId, say "NNN-987643", where NNN is the id of the REMOTE-1 server, to send to REMOTE-1 to identify my account. If I then attempt to authenticate on REMOTE-2, HOME will assign a different networkUserId to send to REMOTE-2. The next time I authenticate on either REMOTE-1 or REMOTE-2, HOME will send the corresponding networkUserId it generated for my first authentication on that remote server. This allows the home server to unlink a customer from one or all networkUserIds, should there be a desire to do so, and blocks attempts by REMOTE-1 and REMOTE-2 to combine data about me.

## HOW DATA FLOWS

The first remote authentication request follows the following sequence:

1. The customer clicks on a link for an article on a remote, in-network, content server (e.g., from a YourSteam email - link actually goes first to YS server and redirects).

2. The remote content server redirects to its authentication server to authorize the request.

3. The remote authentication server puts up its standard login page, with a new "Network Login" button.

4. The Network Login button invokes an ITEGA service controller on the remote authentication server to initiate a remote authentication (networkAuthRedirect.do).

5. The networkAuthRedirect controller saves information about the customer's request (e.g., which article they were asking for) and sends a network authentication request to the ITEGA-Network server via a browser redirect to its networkAuthStart controller.

6. The ITEGA-Network server looks for a cookie it drops with the browser's home server selection. If not found, the ITEGA-NEtwork server displays a page asking the customer to indicate their home server.

7. The ITEGA-Network server redirects the browser to the home server network authentication controller (networkAuth.do).

8. The home server (IdSP) authenticates the customer in its normal manner (which may or may not show a login page) records any information it needs and either finds or generates the appropriate networkUserId for the request. It computes a networkGroupId, based on the customer's current effectiveGroupId. Finally, it redirects back to the ITEGA-Network server's networkLoginStart controller.

9. The ITEGA-Network server drops its home server cookie and redirects to the remote authentication server's networkLogin controller.

10. The remote authentication server locates the original request information, creates a local account, if necessary, maps the networkGroupId to a local effectiveGroupId and continues with its standard authentication process. If the effectiveGroupId is sufficient to authorize the original content request, the remote authentication server redirects to its content server to display the content.

Once the customer has authenticated on the remote server, the remote authentication server can choose to remember this authentication for some period of time, granting subsequent access to content without consulting the ITEGA-Network server.

If the customer has already logged into their home server and has previously authenticated on any remote server so that the ITEGA-Network server has dropped its homeSite cookie, the redirects for authentication will be transparent to the customer. From the customer's perspective, they clicked on an article link in the email and the article appears. In the worst case scenario, such as a browser whose cookies have been cleared, the customer would see the following sequence of pages once they clicked on the article link in the
email:

1. The remote authentication server's login page with the "Network Login" button.

2. The ITEGA-Network server's "Select Home Site" page with a "Submit" button.

3. The customer's home server's login page, where they submit their username and password.

4. The remote authentication server's customer information page, if the site wants to ask the customer for more information.

5. The requested article.

## The NetworkGroupId

The ITEGA-Network  defines a collection of common access properties that servers within the network use to determine which customers have access to which content.

The home servers are responsible for mapping from their own access groupIds to the network groupIds. The remote authentication servers are responsible for mapping network groupIds to their local access groupIds.

The system initially supports the following group Ids, which can be combined as appropriate. Additional groups may be added as desired:

| Bit | GroupId | Name | Description |
|---|---|---|---|
| - | 0 | Anonymous Customer | Customer accessing the site without having logged in (e.g.,  using  a pre-reg meter) |
| 0 | 1 | Group Account Customer | Customer logged in using a group locked account (e.g., IP or accessKey access) |
| 1 | 2 | Registered Customer | Customer logged into an individual non-locked account |
| 2 | 4 | Print Subscriber | Subscriber to print edition |
| 3 | 8 | Digital Subscriber | Subscriber to replica digital edition |
| 3 | 8 | Web Subscriber | Subscriber to online content |
| 4 | 16 | Data Subscriber | Subscriber to special content |
| 10 | 1024 | Comp Subscriber | Subscription is complementary |
| 11 | 2048 | Controller Subscriber | Subscription is granted as a controlled (free) subscriber |
| 12 | 4096 | Paid Subscriber | Subscription requires payment |
| 13 | 8192 | Trial Subscriber | Temporary trial subscription |
| 14 | 16384 | Site Subscriber | Subscription as part of a group (e.g, corporate, university, or library access) |