

UA Measurement WG Meeting

29 November 2021

Attendees

Nabil Benamar
Georgia Osborn
Jim De LaHunt
Ejikeme Egbuogu
Sarmad Hussain
Seda Akbulut

Agenda

1. Welcome and roll call
2. What to take up next: Single sign-on solutions
3. AOB

Meeting Notes

SOW - Popular web hosting tools

Draft SOW for popular web hosting tools is approved by the attendees. A comment access link to the SOW document will be included in the email for others to provide recommendations. Also, a pdf file will be attached.

As a next step, the draft SOW document will be shared in the mailing list with the Measurement WG members. After receiving the inputs, we will finalize it and share with the Coordination WG. After receiving their inputs, we will update and take it further to the Leadership Team for their review and approval. After the approval, it will be posted on ICANN Wiki SOW page.

Single Sign-on (SSO) Solutions

The group decided to take up the work of UA readiness of Single sign-on solutions as a next step, as these are gateway to many services on the web. This topic was previously discussed in the Measurement WG. Many organizations such as Google, Facebook, ICANN, Microsoft use such solutions. And most of the time, these products require email addresses to identify the human being underneath the single sign-on account.

We drafted a new document to outline this new area of work, of which the details are added to the [end of the meeting notes](#). The current version of the document is located [here](#).

Basically, the scope of the work, why it is important to study single sign-on services, and how it promotes the UA were identified.

We reviewed a set of products. The name of the products will be decided in next meetings. We aim to select from a variety of options, that are commercial, proprietary, free, open source, mobile and desktop platforms in different operating systems (Linux, MacOS, Windows, Android, iOS).

Test plan: If the website is not UA ready, but the single sign-on product is UA compliant, how we will know that it is a failure on the website layer, or product layer.

The vendor may need to set up a few websites to test the products. This way we can identify non-UA ready products if the website is UA ready, but the email address fails to sign in through the single sign-on product.

Alternative names: SSO is not the only name for such services. We should find a more generic name that is widely used. Whether these terms refer to the same thing or just try to catch the attention of more web searches needs to be clarified. It will also be consulted to the ICANN IT Team.

The agenda of the next meeting was identified as identifying the name of products we want to include in the SOW in phase 1 at least. The group is also planning to build a testing plan in the next meeting.

Next meeting: Monday 13 December 2021 UTC 1500-1600

Action items

No.	Action Item	Owner
1	Sharing the SOW for popular web hosting tools with Measurement, Coordination WG	Nabil
2	Talking to ICANN E&IT that implemented SSO to get their insights and know more about the difference between similarly named SSO services	Sarmad

UA readiness of Authentication Providers

Scope of Work: Identity platforms

Why is it important to study single sign-on services?

It is used to access many applications including ICANN Account, Google, Facebook, Github, etc. It is a gateway to many online applications.

Psychological impact of the practical usage of EAI: If the email address is rejected, the internet users either give up on using their email addresses and move back to limited-Latin email addresses, or they give up on using the service. We want the users to be able to use their globally inclusive email addresses and never have to make a choice between using the service and using their email addresses. We want them to be able to do both.

Opening the single sign-on services to globally inclusive email addresses will open the door to removing the conflict between many services and globally inclusive email addresses.

How does it promote UA?

Usually, it requires an email address for authentication.

Even if the website users are trying to access is UA ready, if the single sign on tool is not UA ready, it creates an impasse.

What products do we want to test?

- Commercial vs open source
- Free / proprietary
- Desktop / mobile platforms (Android,iOS)
- Different OSs (GNU/Linux, Windows, MacOS)

How many tools?

- Phase 1:** a few tools to better understand how the testing plan works.
- Phase 2:** based on the experience, increase the number of tools to be tested.

Top10 SSO Solutions (<https://expertinsights.com/insights/top-10-single-sign-on-solutions-for-business/>)

Duo Single Sign-On | Ping Identity | CyberArk Workforce Identity | Lastpass Enterprise | Microsoft Azure Active Directory | Okta Single Sign-On | OneLogin Secure Single Sign-On | RSA SecureID Access | SecureAuth Identity Platform | Symantec VIP Access Manager SSO

Top 20 Identity Management Software (<https://financesonline.com/identity-management/>)

Microsoft Identity Manager Microsoft Azure Active Directory Oracle Identity Management Okta Identity Management Zoho Vault OneLogin LogMeIn Pro	Auth0 ExcelID ADManager Plus Centrify Identity Service Intermedia AppID Enterprise RSA SecurID WSO2 Identity Server	ForgeRock Identity Platform miniOrange NetIQ IDM SailPoint Imprivata OneSign DigitalPersona
---	---	--

The 10 Best Free and Open Source Identity Management Tools

(<https://solutionsreview.com/identity-management/the-10-best-free-and-open-source-identity-management-tools/>)

OpenIAM Apache Syncope Shibboleth Consortium WSO2	MidPoint Soffid Gluu	Keycloak FreeIPA Central Authentication Service (CAS)
--	----------------------------	---

Test plan

If the website is not UA ready, but the single sign-on product is UA compliant, how will we know that it is a failure on the website layer, or product layer?

Vendor may need to set up a variety of websites that accept EAI to sign in to those to ensure that the problem is caused due to the SSO tool.

Test each SSO product to log in to the website with multiple versions of email addresses (with combination of “ASCII / Unicode @ ASCII / IDN”, and RTL and LTR)

Another feature is that these products interact with multiple websites for a user. So, it remembers/stores each email address as well the URL of those websites.

We're asking the vendor to do the test integrations of the authentication provider, in order to check that it works. We also expect the vendor to make progress by contacting the authentication provider directly and ask how we can demonstrate that their service works with globally inclusive email addresses and internationalized domain names. The vendor needs to ask the provider if they have a test bed of some sort. So, the vendor will act like a website developer.

-Test if the SSO product is enabled to sign in to the website (New gTLDs / IDNs) with EAI.

-Test if the SSO product remembers/ EAI and New gTLDs / IDNs.

-Test if the SSO product can work with all type of URLs in its own systems.

Related thing to evaluate is Open Authentication, “**OAuth**” <https://en.wikipedia.org/wiki/OAuth>. This is a standard, and a design structure that the identity providers integrate into the products.

In SOW we can ask vendor to evaluate the implementation of OAuth, and in particular look at whether the OAuth standard itself allows UA. In addition, we can ask the vendor to evaluate whether this implementation allows UA. There may be other standards though. (Auth 1.0 and 2.0 are related with these RFCs: RFC 5849, RFC 6749)

We will need to look at the underlying RFCs to see if there are limitations for UA. For example if it refers only to ASCII, then there is nothing to do with the software but with the structure it has integrated.

Alternative names for the service, in addition to “Single Sign-on”:

1. Single Sign-On Solutions
2. Identity Platform
3. Identity Management Software
4. Access Management Software
5. external authentication providers (<https://docs.microsoft.com/en-us/aspnet/core/security/authentication/social/?view=aspnetcore-6.0>)
6. Identity Provider (https://csrc.nist.gov/glossary/term/Identity_Provider),

Other resources:

Auth0 says, “The 2021 State of Secure Identity report is here”:

<https://auth0.com/resources/whitepapers/state-of-security-identity-report> . (This is more about security, which is not our main concern.)

More background reading: https://en.wikipedia.org/wiki/Identity_provider