Universal Acceptance

Work Item: Measuring Universal Acceptance (UA) Readiness of Popular Identity Platforms

Ver.: 2022-03-28

Purpose

This work will test the UA readiness of the Identity Platforms which are commonly used to authenticate the users for accessing websites, systems and applications with their own accounts. The aim of this work is two-fold. The first one is to develop a testing methodology to assess such identity tools, including a validation by using it on two test subjects. The second is to make a small start towards testing the UA readiness of popular identity platforms. Future contracts will apply the test plan to a larger set of identity platforms.

Identity platforms are used to access many applications including accounts for ICANN, Google, Facebook, Github, etc. They are gateways to many online applications. Usually, they require an email address for identification. The technical impact of the email address used here can be described as follows. Even if the website users are trying to access is UA-ready, access to the webpage is blocked if the identification (often known as single sign-on) tool is not UA ready and cannot support an internationalized email address.

There is also a negative impact on the practical usage of Internationalized Email Addresses (EAI) and email addresses with long TLDs in these platforms. If a user's email address is rejected, the user may either give up on using their EAI email address, and move back to an ASCII email address with short TLDs, or they may even give up on using the service.

UASG aims for the users to be able to use their globally inclusive email addresses (including EAI) and never have to make a choice between using the service and using their email addresses. They should be able to do both. Opening the identity platforms for all email addresses and domain names will open the door to removing the conflict between many services and globally inclusive email addresses.

- UA Working Group proposing the work item: UA Measurement WG
- Reference to the Action plan: FY22
- Reference to work item(s): M2

Description of Work

The project will consist of four parts.

1. The vendor is required to come up with a test plan.

2. The vendor uses the test plan to conduct a pilot study to determine the UA-readiness of one commercial and one open-source identity platform that use “OAuth'' standard. Vendor shall choose one test candidate between Okta and Auth0, and one among OpenIAM, Apache Syncope, or Shibboleth Consortium. The vendor shall select and shortlist the candidates in their proposal explaining the reason for the shortlisting.

   In addition to the selected Identity platforms, the proposal will include information about the operating system, browsers, and hosting software for the mail server, which will be used in the tests.

3. The vendor shall attempt to report bugs to the platform provider.

4. The work requires evaluating the implementation of OAuth, particularly looking at whether the OAuth standard itself allows UA.

Project plan

1) Developing a test plan

A detailed testing plan and test cases will be developed based on UA relevant use cases, for review and feedback from the community. The test cases should include all major uses of the identity tools which deal with input, validation, processing, storage and display of the different categories of domain names and email addresses identified as relevant for UA (including domain names with new TLDs, long TLDs, IDNs, and email addresses with Unicode@IDN and Unicode@ASCII-domain-name). Some additional details of the testing are available in the UA Readiness Framework report (UASG026), and example the test domains and email addresses in various scripts are included in UASG004 (associated data file). The email addresses used for testing should cover a variety of cases and scripts.

We're asking the vendor to do the test integrations of the identity providers, in order to check that it works. After testing, a brief report should be compiled to share the test results, along with the detailed testing reports (as appendices in separate files) which can guide website developers which tools to use and how to best configure them to be UA-ready.

2) Test Identity platforms with email addresses and domain names

The vendor shall set up a variety of UA-ready websites at a variety of internationalized domain names (New gTLDs and IDNs in at least five scripts) and email addresses to simulate the UA readiness issue at the website layer and product layer using two or three different browsers (depending on platforms). These websites ideally accept multiple versions of email addresses (with

combination of “ASCII / Unicode @ ASCII / IDN”, and RTL and LTR) to sign in to each identity platform to ensure that the problem is caused due to the identity platform.

The vendor is required to do the tests by logging into the created websites from both desktop and mobile phone.
Apart from testing the user’s email address on identity platforms, another feature to be tested is domain names. These products interact with multiple UA-ready websites for a user. So, it remembers/stores each email address as well as the URL of those websites. The testing plan will include if the identity platform can store / remember EAIs and URLs. However, whether to sign in with all varieties of email addresses will be a separate test.

The details of this plan should be included in the proposal.

3) Reporting bugs to providers

The vendor will also contact the identity provider directly and report any bugs and fixes needed to support globally inclusive email addresses and all valid domain names including the internationalized domain names (IDNs).
-The UA related bugs found should be reported through each identity platform’s bug reporting interfaces online.
-Test if the identity platform is enabled to sign in to the website (New gTLDs / IDNs) with EAI.
-Test if the identity platform remembers/stores EAI and New gTLDs / IDNs.
-Test if the identity platform can work with all types of URLs in its own systems.

4) Evaluate the OAuth standard

The underlying Open Authentication standard, “OAuth” https://en.wikipedia.org/wiki/OAuth will also be evaluated for UA readiness. This is a standard and a design structure that the identity providers integrate into the products. The complete set of RFCs and additional documents to be reviewed should be listed in the proposal.

Deliverables

Based on the work summarized above, the contractor will provide the following deliverables:

1. Draft test plan and detailed test cases for testing UA readiness of identity platforms.
2. Final test plan and test case suite for testing UA readiness (spreadsheet with test cases) incorporating community review.
3. Detailed test report, including the tool versions tested and enough details to permit another tester to reproduce the results.
4. Report on OAuth standard identifying any UA barriers.
5. Draft report on UA readiness of identity platforms, including the following
    a. Executive summary.

   b. Tools and their configurations tested.
   c. Scope of UA testing and summary of test cases.
   d. Summary of the methodology used for testing.
   e. UA readiness of these tools in different configurations, covering Unicode processing, IDNs and EAI support, as listed above.
   f. Survey of other popularly used identity platforms (this section is intended to set the basis for follow up work in this area)
   g. Recommendations
      i. for web developers to select tools and configurations.
      ii. for consumers for selecting UA-ready identity platforms.
      iii. OAuth standard where improvements can be developed.
   h. Conclusions.
6. Final report integrating the community input on the draft report.
7. Presentation (for use as training material) (using UASG PowerPoint template provided) covering the contents of the report, with explanation of testing and observations. In developing the training material consider the following:
   a. Purpose: Provide a high-level reference of the test plan, methodology, process, results and observations.
   b. Target audience: Technical manager (i.e. high level audience). Knowledgeable about Identity Platforms.
   c. Length: The material should be constrained to no longer than 45 minutes, measured by the time one person (within the target audience) would reasonably be expected to need to review the material at his/her own pace
8. Summary of the bug reporting done for the identity platforms based on the testing conducted.

Timeline

- Tentative start date: Date of signing of the contract.
- Tentative end date: Three months of the contract start date.

Conflict of Interest

To help avoid any perceived or actual conflict of interest (COI), UASG leaders, UASG Ambassadors, members holding working group's leadership positions in the UASG, and any organization(s) affiliated with individuals in these UASG roles, are prohibited from participating in this SOW. In addition, ICANN org COI applies.

Proposal Submission

The proposal should include the expertise of the organization with identity platform configurations being proposed (with justification), a high-level test plan (based on use cases) which demonstrates the expertise available and understanding of the UA related issues. The proposal should be submitted to: UAProgram@icann.org before the submission due date.

References

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

UA Readiness Framework report (UASG026)
Test domains and email addresses in various scripts UASG004 (data file)
EAI Software Test Results UASG030A

To refer to previous documents, see document inventory: https://uasg.tech/wp-content/uploads/documents/UASG000-en-digital.pdf