Expression of REFEDS RAF assurance components for identities derived from social media accounts

Publication Date	2018-03-04 (Final)
Authors:	David Groep;Jens Jensen;Mikael Linden;Uros Stevanovic;Davide Vaghetti
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	TNA3.3
Lead Partner:	Nikhef
Document Code:	AARC-G041

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract

Infrastructure Proxies may convey assurance information derived from multiple sources, one of which may be 'social identity' sources. This guidance explains under which conditions combination of assurance information and augmentation of identity data within the Infrastructure Proxy should result in assertion of the REFEDS Assurance Framework components "unique identifier", and when it may be appropriate to assert the "identity proofing" component value low.

Table of Contents

1. Introduction

The Infrastructure Proxies that are a key feature of the AARC Blueprint architecture [AARC-BPA] typically convey user information that has an authentication assurance derived from multiple sources, i.e. is the result of a "combined assurance evaluation" by the Infrastructure Proxy. In interoperability scenarios, the proxy is expected to associate an assurance profile with the authentication assertion provided to its 'customers', and, when required, to assert the assurance component values defined in the REFEDS Assurance Framework [RAF] specification.

In the cases where the Infrastructure Proxy has derived the authentication in whole or principally from 'social media' identity providers (such as Google, Facebook, LinkedIn, etc.), the assurance profile provided with the authentication assertion will usually be "AARC-Assam" (as specified in [AARC-G021]) – although nothing precludes the proxy from using supplemental business processes and combinations that might result in other assurance profiles.

Yet when the primary source of identity is social, and no additional information is available, the question arises whether any of the specific assurance components specified in the REFEDS RAF are also applicable. In particular this concerns the 'unique identifier' (ID/unique) and the identity vetting component based on provided-email-address only (IAP/low).

2. Social media account qualities

Many social media providers encourage unique, non-duplicate identifiers that are associated with real people. In particular Facebook and LinkedIn publish a policy that would make both duplicate and 'fake' accounts a violation of the terms of use. Yet in practice we observe that there is a large fraction of duplicate accounts (up to 10% even in Facebook, which stipulates a one account per person requirement explicitly in its terms and conditions[1]) and accounts not related to real known people (up to 3% in Facebook). Obviously there may also be more than one person with the same name.

However, not all social media, email, and service providers are similarly diligent regarding identifier assignment, and may - for business or other reasons - re-assign identifiers after

[1] See e.g. page 7 in the Facebook statement of Q3 2017, <https://s21.q4cdn.com/399680738/files/doc_financials/2017/Q3/Q3-'17-Earnings-call-transcript.pdf>: "*This quarter, we implemented a new methodology to help identify duplicate accounts. As a result, we increased our estimates for duplicate accounts to approximately 10% of worldwide MAUs from our previously disclosed estimate of 6%. Duplicate accounts are those that we believe are used by the same person and represent real activity and engagement on Facebook.*
We have also increased our estimate for inauthentic accounts to approximately 2-3% of worldwide MAUs. Inauthentic accounts are largely those that are used for spam and other policy-violating reasons."

deletion or a period of inactivity. Such providers include Yahoo[2], Microsoft outlook (hotmail)[3], and GitHub[4]. In these cases, the identifiers provided by that service have only point-in-time uniqueness: these cannot be used for asserting ID/unique, and should not be used for accounting linking in Proxies unless in continuous use without any period of inactivity (identifier re-assignment can happen within 30 days for e.g. Yahoo, so any period of inactivity longer than a 30-day period may imply a change of ownership).

Thus for each social ID provider care is needed to assess their terms and conditions, and changes to the terms and conditions must be monitored by the Proxy.

Neither duplicates nor non-personal accounts would pose much of an issue to an Infrastructure when the social account is used as an authenticating factor to an identified persona already known in the Infrastructure or community: by implication, there is an identity associated with a known person. In all these cases, then, we shall refer to the account as a known “Infrastructure identity”, which in itself will have the properties required in the REFEDS RAF from a “unique identifier”, namely:

1. *User account belongs to a single natural person*
2. *The person and the credential they are assigned is traceable i.e. the CSP knows who they are and can contact them*
3. *The user identifier will not be re-assigned*
4. *The user identifier is eduPersonUniqueID or one of the pairwise identifiers recommended by REFEDS*

In particular requirement (2) can then be satisfied based on Infrastructure and community registries. To meet requirements (1), even in this case additional controls may be necessary. These controls can take the form of a policy statement, e.g. by adding to the infrastructure AUP that "I won't use a shared account to log in or disclose my credentials to anyone" and to some extent count on the implicit understanding by qualified Infrastructure users that accounts and authenticators are valuable. Excluding bots should be relatively easy: first, captchas tend to do a good enough job even if they annoy legitimate users, and second, while bots can join mailing lists, they have not yet, as far as we know, evolved the sophistication to join research communities and access services through CSPs.

In absence of additional information to support (1), for Infrastructure identities whose accounts are solely backed by social media identity sources and nothing else, the basic

[2] “*Our goal with reclaiming inactive Yahoo! IDs is to free-up desirable namespace for our users. [...] We will have a 30-day period between deactivation and before we recycle these IDs for new users. During this time, we’ll send bounce back emails alerting senders that the deactivated account no longer exists.*” Quoted from a statement given to Wired, cited at https://www.pcworld.com/article/2042508/yahoo-tells-security-critics-to-chillax-regarding-its-email-recycling-program.html, visited March 2018.

[3] The Microsoft Services agreement requires users to log in at least every 270 days. In a statement by Microsoft to WebWereld.nl, it confirms “*that these email accounts are automatically placed in a queue on our servers and scheduled for deletion. Then, after in total 360 days, the email account name will be made available again.*” Quoted by WebWereld (in Dutch), http://webwereld.nl/security/79529-microsoft-recyclet-stilletjes-outlook--en-live-accounts, visited March 2018.

[4] While account uniqueness in a precise moment in time is granted, GitHub accounts are re-assignable after deletion, see https://help.github.com/articles/deleting-your-user-account/

requirements of REFEDS RAF “ID/unique” cannot be met. Based on the publicly known account qualities, and without compensatory controls, neither (1) “single natural person” nor (2) “… the CSP knows who they are …” can be satisfied. The duplicate accounts are not a critical issue in this respect, but particularly (2) would not be compatible with fake accounts, that are not ‘known’ to the credential service provider without linking to another identity or identifier.

Additional heuristics can be applied by the Proxy to help meet these requirements. One valid option would be to verify control over a personal email address associated with a well-known and reputable organisation (e.g. the users home university or research institute on a managed domain, which would allow users with an institutional email address but no institutional IdP that releases attributes to participate in the Infrastructure). Such heuristics could even include behavioural analysis, or take other forms. The business logic thereof is to be determined by both technical and policy factors.

Yet without such further processing it would be a violation of the REFEDS RAF specification to include “https://refeds.org/assurance/ID/unique” in the assurance attribute or claim provided by the Proxy to third parties.

3. RAF component recommendations

The above-listed consideration lead to the following guidance on asserting assurance component values:

The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam **DO NOT assert any REFEDS RAF component values**
The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through heuristic or other business logic, that provide additional keys to 'who they are' and that the user is a single natural person and not sharing the account. The social ID itself is never re-assigned.	Assert profile AARC-Assam **ALSO assert** **https://refeds.org/assurance/ID/unique**
The Infrastructure ID is co-based as above, but in addition either the Proxy or an 'upstream' identity source provides a valid email address through which the user can reasonably be expected to be reached	Assert profile AARC-Assam **ALSO assert BOTH** **https://refeds.org/assurance/ID/unique and** **https://refeds.org/assurance/IAP/low**

With this combination, the recipient of assurance information from a Proxy can derive unambiguously the status of an account which is based wholly or partially on social media authentication.

References

RAF https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group
visited 20 February 2018

AARC-G021 *Exchange of specific assurance information between Infrastructures*
AARC Guideline 021, https://aarc-project.eu/guidelines/aarc-g021/