Comments on “Using authenticators to protect an online service”

1. The following phrase is correct, “1.0 You might need to know if someone has already used your service before you give them access to it. This is called 'authentication' and can be useful if users need to sign into your service more than once.”

   However, Kantara suggests that it is an oversimplification as it mixes the concept of authentication and authorization. Kantara defines authentication as the process of validating the identity of a registered user before allowing access to the protected resource and authorization as the process of validating that the authenticated user has been granted permission to access the requested resources.

   In addition, Kantara believes that the phrase implies a relationship between the concept of authentication and the idea of authenticator which is the subject of the guidance document.

   With this in mind, Kantara would suggest the following phrase, “You might want to be sure that someone is who they say they are (i.e., authenticate them) before you give them access it and determine if they are entitled (i.e., authorized) to use it. This important for a single use of your service, it is even more important if a user needs to access your service more than once. Once someone is authenticated they can be given an authenticator they can use to access your service again.”

   While Kantara understands the desire of the UK Government to simplify, it recommends clarity, and in this particular context, over-simplification may incur the opposite. The concepts of authentication, authorization and authenticator are very important and should not be amalgamated and oversimplified.

2. Kantara recommends that RP's use real-time protection against repeated password authentication attacks, like limiting the number of retries before locking an account or at least enforcing an exponential delay on password re-tries. While the UK, like everyone else, is pushing to use stronger authentication methods, passwords remain the overwhelmingly prevalent method in use.

3. Kantara finds the rest of the guidance document to be clear and understandable.

Comments on “Identity providers in the Identity and Attributes Exchange (IAX): what you must do”

1. Numbering of sections and subsections would help with reading and navigating the document.

2. Kantara is now uncertain as to the audience for the guidance. It seems initially to address IDP's (which would be logical given the derivation from the IDV Ops Manual), but in several places it mentions access to the "service you provide," which sounds like the guidance is addressing an information service-providing RP. Kantara doesn’t usually envision the IdP function maintaining a separate account for the user/applicant. Kantara envisions that the IDP provides digital credentials for use in accessing other organizations' information services and, as such, the function doesn’t provide unrelated (to identity) information services. However, given Gov.UK Verify’s use of IDPs that are commercial entities with customer accounts associated with its

business activities, perhaps this is an implicit assumption in the drafting which could be made explicit for clarity? In addition, Kantara recommends the introduction of the term Attribute Provider for the function of providing attributes not related to authentication or authorization.

3. Kantara was confused by the draft's mixing two quite separate functions: authentication / authorization vs. User Interface personalization and whether the guidance was targeted at RPs or IDPs, or perhaps the same entity acting in both these roles. For example, Kantara was unclear whether the "account" mentioned in the draft would be the linked local business account of the consumer at the RP (e.g., their bank account) and not their identity account at the IDP. But again, this could be a manifestation of the implication around the nature of Verify's IdPs.

4. Setting Up a Digital Identity Account section: The collection of additional information (i.e., You can ask the user for more information if you want to personalise the user experience) can have privacy implications. One has to be careful to minimize the collection of information beyond that which is absolutely necessary to establish a unique identity and to manage that identity. Kantara recommends that the guidance be careful about promoting the collection of additional information just for the sake of convenience.

5. Check Information About a User is Accurate section: The lead in to this section, (e.g.,"You must check the information the user gives you is accurate before you let them access services with their digital identity account.) seems to be written from the perspective of a business service rather than an identity provider service. The rest of the section concerns the information contained in someone's digital identity account. But again, this could be a manifestation of the implication around the nature of Verify's IdPs.

6. Closing an Account section: Kantara recommends that the IDP will also want to close an account if it has been determined to have been mis-used.

7. There are a couple of places in the guidance that say that the IDP must "submit a report." Kantara recommends that there be some indication of to whom the report is to be submitted?

8. In order to reduce the opportunity for fraudsters to generate valid-format DL numbers, Kantara recommends removing the detailed description of the DL pattern.