March 2nd 2020

Government Digital Services,
The White Chapel Building,
10 Whitechapel High St,
London E1 8QS

To whom it may concern

Upon receipt of the February 2020 Draft of GPG44 (Using Authentication to Protect an Online Service), Kantara formed a special sub-group of its open community Identity Assurance Work Group (IAWG) to review the document. As part of participating in this sub-group members agreed to both not re-distribute and not discuss the document beyond the work of the sub-group to avoid misconceptions being created about the work in the public domain.

As a result of the work of this sub-group Kantara is pleased to offer the following comments on the February 2020 Draft of GPG44 as emailed to Kantara on February 18, 2020.

Overall Comments

It is unclear at whom the document is targeted. From reading it and GPG45, it appears that the intended audience is providers of on-line services which require authenticated user access, and therefore not providers of proofing and authentication services. That is, using Kantara terminology, it is targeted at Relying Parties (RPs) rather than Credential Service Providers (CSPs). Kantara recommends that the target audience be identified.

If Kantara's assumption is correct, then Kantara recommends that the document should concentrate on "actionable" guidance for that audience. That audience is not likely interested in learning about technology (e.g., "tokens"), but would likely be interested to know what steps they should take and what issues to consider. This is done effectively, for example, in the draft's advice that a risk analysis is a prerequisite for making a decision on the appropriate strength of authentication.

The document seems to assume that in general, the RP will act as its own CSP/IDP. Specifically, there are multiple mentions to the user's "account" (at 1.0, 3.4, 4.3, etc.) which appear to refer to an account at the RP vs. "federated" credentials issued to a user ("subscriber") by an independent CSP/IDP. Kantara recommends more explicit guidance be included to address the federated-

credential use-case, and to distinguish between a user's "account" at an independent CSP/IDP and their linked local (RP) account, if one is required by the use-case.

The document discusses the weaknesses of KBA (often publicly available and also often static) and of biometrics (vulnerable to spoofing and also static) but is generally neutral on using these authenticators. Kantara notes that recent US NIST guidance discourages the use of KBA and is cautious on biometrics (for the reasons cited in the draft.) While Kantara recognizes that different national authorities have different policies, Kantara recommends that some consideration be given to emphasizing the limitations of KBA in particular. Kantara is unsure of what to provide as good example of "dynamic KBA". That being said, Kantara recommends that an example be provided.

Kantara believes that authentication provides two valuable benefits: (1) it provides a basis for seeking recourse (via the credential issuer) if the actions of an authenticated user cause harm; and (2) it provides a selected level of assurance that the user who authenticated and logged in to a system today is the same as the user who did it before. Kantara sees that the latter benefit is cited in the document, but that the former is not. This is perhaps because the document seems to assume that the RP is also the CSP/IDP, in which case the records needed to hold a user accountable are already in possession of the RP.

Kantara recommends that the issue of the cost of different authentication approaches be discussed. While security is paramount, RPs will likely take cost into consideration when making a decision concerning the authentication approach it will use.

Specific Comments

Section 2.2: Kantara recommends that the example provided might be reconsidered. A casual reader might take away from the example that they could manufacture a second authentication factor by writing down a password (underneath the keyboard perhaps). This approach would in fact destroy the value of the password secret; plus there is a presumption that "something you have" authenticators are very difficult to reproduce, unlike a phrase written on a piece of paper.

Section 13.2: This section includes, as a feature of a "medium protection" authenticator set, that "... information (such as bank data in a chip and PIC card) ... has not been tampered with." This seems off-topic (bank data presumably not being related to authentication) and therefore potentially confusing.

Sections 18.1 and 18.2: These sections advise "... look out for unusual activity once [the user has] signed in." Kantara believes that this is not the most straightforward way to discover the "authenticator stuffing" attack used as the example in 18.2. Kantara would suggest that evidence of authenticator stuffing would be a large number of failed attempts, and abandoned after one try, login attempts over a short period of time, and that this would occur before a user has signed in.

Yours sincerely

Colin Wallis

Executive Director
Kantara Initiative Inc, Educational Foundation Inc & Kantara Initiative, Europe
Executive Director
Cell: +44 (0)7490 266 778
@KantaraColin