**Thoughts on progressing the Identity Assurance Service Assessment Criteria (SAC) and Attribute provision:**

***Objective***: This brief paper outlines a series of steps by which the SAC might be developed in a manner which would remove US-centric references within criteria, would be supported by purpose-specific (e.g. corporate or jurisdictional) profiles and which might then provide an avenue by which the SAC could be the basis for criteria addressing attribute provision services. It also discusses how attributes and Id credentials might relate in terms of ALs.

***IPV* versus *attribute provision***: It is important to understand that Identity Proofing & Vetting (IPV) is about establishing (or not) the validity of an identity, at a given AL, whereas Attribute Service Providers (ASP) are binding qualifications or other recognized characteristics (the attributes) to a proven and verified identity. Furthermore, the authoritative sources of attributes, whether the ASP itself or via an Attribute Broker, must themselves have a proven and verified Id in order to be able to be authenticated as the root source of the attribute.

***Approach***: A number of steps can be identified, which are described below in a suggested order of implementation:

1. Irrespective of any changes /modification in the queue for the SAC (i.e. tickets and any other ideas in the pipeline) on an individual criterion basis, an thorough review should be performed to identify which criteria are written in a style which is directly dependent on either a US reference by direct reference or implicitly by the inclusion of a specific piece of text (e.g. references to entropy which derive directly from NIST SP 800-63-2);
2. The CO-SAC could also be reviewed to determine which of its criteria can be considered not COmmon (to CSPs) but perhaps COre to any service which KI might approve (e.g. the stability of the organization and their operational practices). Some comments in the existing CO-SAC are skewed towards CSPs, the original rationale being that they were indeed common to all the elements of CSPs but they would not be applicable to Electronic Attribute Providers (gets the ‘EAP’ back into the loop ;-);
3. Capture of any criteria removed from the (existing) CO-SAC into the OP-SAC, in a form appropriate to however the SAC might, in parallel, evolve to accommodate the final modular approach;
4. Once the CORE-SAC has been developed then that can be common with criteria applied to ASPs, but operational and technical criteria must be separately developed (AP-SAC).
5. Open question: would the AP-SAC criteria need to follow the principle of being non-US-centric, and subject to profiling, as described above?
6. Lastly, need to review what ISO standards may exist or be in development – should we develop in an active partnership (and suffer the implications of that action)?

***Determining an Attribute’s Assurance Level***: This point is considered on the presumption that the ALs of an attribute assertion framework[[1]](#footnote-1) will adopt the ‘standard’ OMB-M-04-04 framework (de-nationalized, of course – perhaps by reference to IS29115) – isn’t this essential in order to marry AAs to Ids?

Given that , then the entity which issues an assertion at ALx must itself have been id-proofed/verified at that same AL or higher, and that requirement goes back to the root issuer, e.g. if a broker is combining attributes and uses an educational qualification from a general board which relies upon an assertion from a specific university, then each of those three entities must hold an id credential at ALx or higher.  One might also suggest that, in principle, the Subject of the attribute assertion must hold an Id credential at ALx OR LOWER (i.e. it would not be permissable or sensible to offer an AA at AL4 for a subject at AL2, since the latter would set the upper confidence level at which the Id is proven and hence the certitude of matching that Id to the given attribute would be limited by that level of confidence in the assurance *per se*).

Beyond that, development of criteria applicable to ASPs would have to draw parallels from the OP-SAC in order to derive comparable rigour. This should include consideration of how ASPs must gain a credential.  We should note that these ASPs will be organizations, not individuals (very likely, at least), and thus far the SAC addresses only the Id-proofing of persons, albeit with a corporate ‘flavour’ by dint of the Subscriber role.  Note that WDIS29003 is (ultimately) going to address persons, organizations, h/w and s/w and presumably the ARB & IAWG will want the SAC to follow suit.

***Trust elevation***: On a final note, the SAC have no accommodation for such practices, which have the potential for application to attributes as much as to Id credentials.

1. is that the ‘AAF’ or do we extend the IAF to be the ‘Identity and Attribute Assurance Framework – IAAF’? Or do we cover all bases and, taking the ‘C’ out of NSTIC, re-name the IAF the ‘[International] Cyber Assurance Framework’? [↑](#footnote-ref-1)