2019-12-05 Meeting Minutes - Meeting with NIST

Attendees

Invited Guests: Jim Fenton, David Temoshok (NIST), Christine Abruzzi.
Non-voting participants: Roger Quint, Pete Palmer
Voting participants: Ken Dagg, Martin Smith, Mark Hapner, Richard Wilsher

Staff: Colin and Ruth

Quorum: 4 of 7. There was quorum

Agenda

1. Administration:
Roll Call
2. Discussion:

a) NIST response to Kantara Implementation Guidance Reports on 800-63-3

b) DIACC Call for Comment on PCTF Verified Login Component Overview & Conformance Profile Draft Recommendations V1.0

Various

- Ken announced that IAWF 1050 Glossary and Overview was approved by All Member Ballot and it will be published shortly.

Discussion on NIST Response - Continuation session

Comments about Kantara Implementation Report Response 090319

Item 2 Impasse on KBV approval for IAL2

- David Temoshok mentioned in relation to the use of knowledge-based verification for identity evidence at the “fair” level for one piece of evidence that it is probably not very helpful, but this is what 63A defines as the requirement for that. He added that there is no further use of knowledge base verification in either, the identity proofing processes for IAL or for authentication processes for AAL. The explanation provided for this, on why such limitations exist is explained in 63-3 as well as in the Response note to Kantara.
- Richard added that Roger pointed out that the problem is finding a proofing path, the problem with IAL2 is when you come to verification, there is no fair evidence that would be used at that stage when you have to have at least one strong.
- Mark expressed that he understood from what was said that for IAL2, that KBV is basically useless. David responded that it is necessary to define “useless”, KBV could always be used by a CSP for further proofing, but it is just not considered one of the required means of identity validation or identity verification, thus you can use KBV as an additional control.
- Martin asked, “Is the data collected for that technique, is that typically considered PII?”, the answer was “certainly”, then it was said that it would represent another risk factor mitigating against using the ISPs wanting to collect that. David said that 63A in further identity proofing for self-asserted identity characteristic is not provided for.

Item 3 Consistency of terms describing proofing types

- Richard has proposed a set of terms for further clarity.
- David made comments on the concepts used in identity proofing and in particular for the presence requirement for identity proofing, presence requirement for IAL2 could be either “remote or “in-person”. The terms “remote” and “in-person” are used as dictionary-defined terms.

-Remote identity proofing, the applicant and the operator or interviewer are remote, it represents an identity proofing session where the CSP and the applicant are in separate locations, not meeting face-to-face, with communications over a network.

-In-person is a face-to-face identity session in the same location between the CSP and the applicant.

-In addition, a new term was introduced in 63A for “supervised” remote in-person identity proofing; it has explicit connotations. “Supervised remote identity proofing” means that the requirements and controls for identity proofing sessions specified in SP 800-63A section 5.3.3.2 Requirements for Supervised Remote In-Person Proofing are applied. SP 800-63A section 5.3.3.2 requires specific physical, technical and procedural controls so that supervised remote identity proofing can be considered equivalent to an in-person identity proofing session and, therefore, meet the in-person presence requirement for IAL3.

- About this, Richard commented that David described “in-person” as the applicant and the CSP being in the same location, and that it was also suggested that there is “remote” where the applicant is in contact there in network connection to somebody on behalf of the CSP. Consequently, it was said that there is a confusion, because there is implied that there are two levels of interaction between the applicant and a human being on the part of the CSP, because now it is said “supervised”. David answered that it is not what he mentioned, the term “supervised” has very special meaning in 63A. He added that “supervised” when we refer to remote identity proofing, which would meet the requirement of in-person identity proofing, but the encounter is remote between the applicant and operator, thus supervised in this context means there is specialized equipment that allows the CSP to be able to view the entirety of the identity proofing session, to be able to check both documents and the entire session to ensure that the applicant is present, they can view the applicant through the entire session and there is no one else present. The specific control in order consider that such a remote process would be equivalent to a "in-person" session, those requirements are covered in SP 800-63A section 5.3.3.2 and are called Supervised Remote Identity Proofing.

- Jim appreciated the input on the terms since it is necessary to be as precise as it is possible. However, he argued that he has some trouble to see something as unsupervised because it kind of implies that it cannot be supervised, and it should not follow into that trap. He considered it is not anything that can be acted on anytime soon.
- Jim also mentioned that you can still have human interaction and still not meet the requirements for supervised because, the difference between "supervised" and "unsupervised" is that "supervised" you may think it is a specific piece of hardware that is conformed be the CSP in order to be proofed. The difference at IAL2 when you are doing proofing that does not involve Supervised Remote Identity Proofing is that interaction could be on the users on PC, they can use a webcam, they may have a voice session if they are interacting with a human agent. He stressed that the difference between "supervised" and "unsupervised" for him is the question of whether there is a location that has a specific purpose made piece of hardware conformed by the CSP, or whether it can be done from an office.
- David stressed that Supervised Remote requires a CSP equipment for the remote applicant.
- Roger said he understands from this perspective that, if the CSP provides the equipment, it does not matter whether if there is a human person reviewing that or not as long as the equipment belongs to the CSP. Jim answered to him that there is a whole set of requirements in order to be able to call it Supervised Identity Proofing and it is not a requirement for IAL2.
- It was asked if the Supervised Remote at IAL2 requires a physical representative of the CSP to be involved during the proofing process. Jim responded that it would not be called like that if it is an IAL2, you can use the same equipment but all of the requirements of 5.3.3.2 do not apply at IAL2, you can use the equipment if it was available and it was convenient for applicants to use that equipment but it is not a requirement at IAL2.
- Richard's proposed table would have to be changed considering the NIST comments and clarification on it.

Item 4 Scope and Application of 'Trusteed Referees'

- Jim thinks that Trusted Referee is an accessibility feature, it is wanted to allow somebody who has a certain disability to get Identity proofed. Given that this is Government to Citizen, we need to make identity proofing available to as many people as possible, so people are not being disqualified for their inability to complete a particular process. The Trusted Referee thing, in different situations, it could be more analogous to a personal assistant that is just helping someone to get through the process.
- David pointed out that the idea of Trusted Referee Process is optional to the CSP, it is not a normative requirement. If the option is chosen, then there are some normative requirements. It is intentionally flexible in 5.3.4, there is not overly specified how this would be provided. He continued that, in the circumstances that Richard indicated, it is someone that is known to the applicant to help facilitate the applicant through the application process. If this were an identity proofing operator or supervisor or any term for the CSP that intends to help facilitate applicants into the process it could be that type of process as well, it could be either of both or potentially both.
- It was argued that those should not be read together, since those are separate requirement; 5.3.4 is optional to the CSP. The CSP is expected to develop their procedures for the use of trusted referees, whether there is somebody that potentially represents the applicant or the CSP provides processes that enable applicant that otherwise would find it difficult to apply, to facilitate the enrollment process.
- The representative is able to meet identity proofing requirement with the CSP in representing the applicant. However, it is conceivable that a CSP could develop procedures where a trusted referee can represent the applicant with the CSP, with identity evidence for representing the applicant to satisfy identity proofing requirements at IAL2.
- It was clarified that that remote operator is distinct from live operator.

- It was agreed to have a next session to continue discussing the pending points (e.g. report #5).

DIACC call for comments on PCTF documents

- Ken commented that DIACC released an updated version of Verified Login Component of the Pan Canadian Trust Framework (PCTF), where some of IAWG comments were accepted. See: Comments to DIACC on PCTF Verified Login Component and Conformance Profile v1.0
- It was agreed to release an eBallot to determine if IAWG will develop comments on the updated version of Verified Login Component of the Pan Canadian Trust Framework (PCTF).
- Deadline to comment January 20th.

Revision of Glossary and Overview in light of IS17065

- It was agreed to defer this discussion to end of January.

Action items

- Schedule a new discussion session with NIST.