Kantara Implementation Guidance Report

**ID:** 2019-Z-02 ver. 2.0

**Subject:** Scope and Application of ‘Trusted Referees’

**Date:** 2019-06-27-  
**To:** Kantara Assurance Review Board, Kantara Identity Assurance Working Group

**CC:** NIST, GSA

**From:** Zygma Inc.

**Background:**

A number of CSPs use the term ‘Trusted Referee’ (‘TR’) in the context of a CSP representative who oversees Supervised Proofing (see Implementation Guidance report 2019-K-01), and the term is being more broadly adopted with this usage. The scope of a TR is however muddied by some implications of the associated requirements and other terms used less forcefully/formally. This report analyses these usages and proposes terminology for Kantara’s application in its criteria and for CSPs, Assessors, RPs and Kantara’s various bodies, to ensure consistency.

**Analysis:**

In NIST SP 800-63-A two clauses define the requirements for using a Trusted Referee (‘TR’). This is not a term defined in SP 800-63-3, so this is all the definition we are given. (The text of this report capitalizes it for the sake of emphasizing that it should be considered to be a defined term.)

### 4.4.2 IAL2 Trusted Referee Proofing Requirements

In instances where an individual cannot meet the identity evidence requirements specified in Section 4.4.1, the agency MAY use a trusted referee to assist in identity proofing the applicant. See Section 5.3.4 for more details.

…

Note that ‘the agency’ MAY use a TR, not in this case the CSP. No-one has taken this to be a denial of use of TRs by CSPs, who are actively openly engaging the concept, assessors are accepting the concept and the ARB are approving services embodying such service aspects. The continuing requirements then provide some formal understading of what a TR is:

### 5.3.4 Trusted Referee Requirements

1. The CSP MAY use trusted referees — such as notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals — that can vouch for or act on behalf of the applicant in accordance with applicable laws, regulations, or agency policy. The CSP MAY use a trusted referee for both remote and in-person processes.
2. The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.
3. The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing. In addition, the CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.
4. The CSP SHOULD perform re-proofing of the subscriber at regular intervals defined in the written policy specified in item 1 above, with the goal of satisfying the requirements of Section 4.4.1.

Note that §4.4.1 is titled ‘IAL2 Conventional Proofing Requirements’. This is the sole use of the word ‘Conventional’ in this entire part of SP 800-63 rev.3. It is essentially noise.

On an initial reading one might think that this TR is someone known to the applicant, a practice which arises in certain conditions and which should not be disregarded. However, phrases such as ‘*notaries’* and ‘*other ... trained and certified or approved individuals*’ give great latitude to the extent of prior relationship between the TR and the Applicant, and could equally support an argument that there need be none whatsoever prior to the proofing event at which the TR acts in some capacity to facilitate the proofing. Again, the agency/CSP is given liberty to define the requirements for a TR and the nature of their relationship or association to the Applicant.

However, 800-63-a makes other references to someone having responsibility for overseeing Supervised Proofing in the following excerpted and highlighted clauses:

### 5.3.3 In-Person Proofing Requirements

In-person proofing can be satisfied in either of two ways:

* A physical interaction with the applicant, supervised by an operator.
* An [sic] remote interaction with the applicant, supervised by an operator, based on the specific requirements [Section 5.3.3.2](#fivepointthreepointthreepointtwo).

And within this section, as follows:

#### 5.3.3.2 Requirements for Supervised Remote In-Person Proofing

CSPs can employ remote proofing processes to achieve comparable levels of confidence and security to in-person events. The following requirements establish comparability between in-person transactions where the applicant is in the same physical location as the CSP to those where the applicant is remote.

Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in [Section 4.6](#fourpointsix):

1. The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.
2. The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.
3. The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.
4. The CSP SHALL require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.
5. The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a virtual in-process proofing session.

So we know that an operator who is both live and remote in one case has to supervise. Can this operator be a TR? One interpretation could be that, since the term ‘trusted referee’ is not used, there is an intention that they be different. Another could be that different authors of these sections failed to join their respective dots. Other inconsistencies in the publication suggest the latter may be nearer the truth.

**Conclusion & Recommendations:**

Given the vagueness of the requirements and the mixed terms used, one could conjecture on a TR being realized in two different ways. One is where the TR has antecedent knowledge of the applicant, e.g. is the applicant’s neighbor, accountant, physician, … In this case, the TR is more of an Applicant’s Referee who would act on behalf of the applicant to persuade the proofing CSP as to the applicant’s claims of identity being true.

The other case is where the TR has no antecedent knowledge of the applicant and is acting on behalf of the CSP (and potentially an agency, where that is managed by the CSP).

It seems reasonable that in either case the TR must be identity-proofed and subsequently authenticated to the same IAL/AAL as the proofing process which they are required to support, and that all other considerations (e.g. policy defining how to use them, training in some cases) be defined in each case. However, that requirement could easily dissuade an Applicant’s Referee from acting in that capacity, simply because of the hassle.

Based on the foregoing, Zygma recommends that the IAWG adopts and applies the following interpretation of the SP 800-63-A requirements and that NIST is made aware of these interpretations such that it can amend 63-A accordingly.

**Recommendation 2019-Z-02#1:**

That the IAF adopts the following interpretation of the SP 800-63-A requirements as follows:

1. the term **Trusted Referee** be used in a broad context, if required at all, embracing the two specific terms described in items ii) and iii) below;
2. the term **Applicant’s Referee** be introduced and used exclusively when a Trusted Referee is acting on behalf of the applicant;
3. the term **Supervisory Referee** be used exclusively when that individual is acting on behalf of the CSP (or agency);
4. the clauses of SP 800-63-A §5.3.4 be applied to the distinctive TR types as follows:

|  |  |  |
| --- | --- | --- |
| **§5.3.4 sub-part** | **Applicability to Applicant’s Referees** | **Applicability to Supervisory Referees** |
| 1) | Applicable as stated | Applicable as stated |
| 2) | “The CSP SHALL establish written policy and procedures as to how a trusted referee is determined” Nothing else is required since this is a ‘one-off’ intervention | Applicable in full |
| 3) | Applicable as stated, though the binding relationship SHALL be based on antecedent characteristics which demonstrate a pre-existing relationship of substance. | Applicable as stated, though the binding relationship shall be determined through adherence to policy, process and with appropriate training. |
| 4) | Not applicable | Amend to read: “The CSP SHOULD perform re-qualification of the Supervisory Referee at regular intervals, as defined in the CSP’s CrP.” |

1. the two references in SP 800-63-A §5.3.3 to ‘an operator’ be replaced with ‘a Supervisory Referee’;
2. the references in SP 800-63-A §5.3.3.2 to ‘live operator’, ‘remote operator’ and ‘operator’ each be replaced by ‘Supervisory Referee’;
3. criteria in 63A\_SAC be revised accordingly to reflect the usage of these terms and the applicability of §5.3.4 sub-parts as described above;
4. terms to be added to the Kantara IAF Glossary.

**Recommendation for Kantara:**

It is noted that SP 800-63-A §4.1 is titled ‘Identity Assurance level 2’. It therefore appears that there are no ‘TR’ requirements for IAL3 – is this to be taken as an oversight or as an attempt to deny by omission such entitlements at IAL3? Since the 63A\_SAC addresses only IAL2 this could be a bridge to be crossed at some time in the future, though the following recommendation is offered:

That at IAL3 all (Applicant’s and Supervisory) TR requirements are applied as stated for IAL2 unless there is any conflicting or overriding IAL3 requirement, the (presumably) greater rigour of which SHALL be applied.

**Request to NIST**:

Please review the above and provide the community with a formal response against which application of SP 800-63 rev.3 can be confidently effected, e.g.in the form of an erratum to the necessary clauses of the suite as a whole.