Comparison of SAC 058, NIST, EU, and Edgemoor identity scales

Steve Crocker, 5 October 2021

This is a quick comparison of the identity scales in ICANN SSAC’s SAC 058, NIST SP 800-63a Digital Identity Guidelines, and EU eIDAS Regulation (2016). The relevant texts are copied below.

Caveat: I have not followed the developments of each of these scales. This comparison is based on my quick reading of the texts. This note is provided for review and discussion. Comments, criticisms, corrections, etc. are welcome.

## Introduction

An identity specification consists of a number of data elements, e.g. name, country, city, street address, phone number, email, etc. that are correlated with a specific person. In principle, if this data is accurate, it should be possible to find and/or contact the indicated person. In practice, even if the data is accurate the person may not be findable or reachable. For example, the person may not be at the location indicated or the person may not answer a phone call or email message.

The data elements are presumably acquired during a registration process based primarily on data supplied by the registrant. In some settings, some of the data elements may be acquired by indirect means.

The scales are intended to provide a basis for confidence (or lack of confidence) that the data is accurate.

The NIST and EU scales apply to the full collection of data elements and address the confidence level of the entire data set. The SSAC scale is applicable on a per data element basis. Further, the SSAC scale is phrased in terms of operational tests applied to the data elements. The NIST and EU scales are phrased in more general terms.

Edgemoor Research Institute (ERI) is using the SSAC scale, augmented with an additional notation to indicate no validation.

## Comparison

The SSAC scale is stated on a per data element basis. The NIST and EU scales apply to the collection of data elements associated with an identity.

The following table is my best guess at how these scales align with each other.

|  |  |  |  |
| --- | --- | --- | --- |
| ERI | SAC 058 | NIST | EU |
| V0 |  | IAL1 | Low |
| V1 | Syntactic |  |  |
| V2 | Operational |  |  |
| V3 | Identity | IAL2 | Substantial |
| IAL3 | High |

## Text from each of the documents

### ICANN SSAC SAC 058

The SSAC asserts there are three types of validation for elements of the registration data.[[1]](#footnote-1)

1. Syntactic Validation refers to the assessment of data with the intent to ensure that they satisfy specified syntactic constraints, conform to specified data standards, and are transformed and formatted properly for their intended use. For example, if the data element is expected to be an email address is it formatted as an email address? In general, it is expected that syntactic validation checks would be entirely automated and could be executed inline with a registration process, follow up information reviews, and whenever registration data changes.

2. Operational Validation refers to the assessment of data for their intended use in their routine functions. Examples of operational validation include 1) checking that an email address or phone number can receive email or phone calls; 2) checking that a postal address can receive postal mail; 3) checking that the data entered are self-consistent, i.e. that all data are logically consistent with all other data. It is expected that many operational validation checks would be automated and some could be executed inline with a registration process.

3. Identity validation refers to the assessment that the data corresponds to the real world identity of the entity. It involves checking that a data item correctly represents the real world identity for the registrant. In general, identity validation checks are expected to require some manual intervention.

### NIST Levels

Assurance in a subscriber’s identity is described using one of three IALs:[[2]](#footnote-2)

**IAL1:** There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject’s activities are self-asserted or should be treated as selfasserted (including attributes a CSP asserts to an RP). Self-asserted attributes are neither validated nor verified.

**IAL2:** Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL2 can support IAL1 transactions if the user consents.

**IAL3:** Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained CSP representative. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL3 can support IAL1 and IAL2 identity attributes if the user consents.

### EU Levels

The three levels of assurance are as follows:[[3]](#footnote-3)

* **Low**: for instance, enrolment is performed by self-registration in a web-page, without any identity verification;
* **Substantial**: for instance, enrolment is performed by providing and verifying identity information, and authentication by using a user name and a password and a one-time password sent to your mobile phone;
* **High**: for instance, enrolment is performed by registering in person in an office, and authentication by using a smartcard, like a National ID Card.
1. <https://www.icann.org/en/system/files/files/sac-058-en.pdf>, section 3, pages 7-8 [↑](#footnote-ref-1)
2. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>, section 2.2, page 3 [↑](#footnote-ref-2)
3. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+assurance [↑](#footnote-ref-3)