IIF (IUCC Identity Federation)

Level of Assurance

Authors	Zivan Yoash, Yossi Baruch, Arad Alper
Last Modified	02.12.2014
Version	1.0

Table of Contents

1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119.

2 Purpose and Scope

This document defines the lowest common level of assurance required for all members of the IUCC Identity Federation (IIF). This identity assurance profile does not represent LoA 1 in the sense of NIST SP 800-63, but should rather be thought of as an 'unspecified' LoA. A claim at this level of assurance implies roughly the following:

- The subject is probably affiliated with the IIF member
- The subject is very likely a human and not a robot or piece of software
- The subject is most likely identified by a unique permanent user identifier
- Relying parties in IIF may require elevated levels of assurance.

3 Compliance and Audit

Evidence of compliance with this profile MUST be part of the Identity Management Practice Statement, maintained as a part of the IIF membership process. No audits are required for this identity assurance profile.

4 Requirements

4.1 Organisation

- The organisation operating the identity provider MUST be a part of the IIF member organisation or under contract with an IIF member organisation.

4.2 Identity proofing and registration

- All subjects MUST at least with some degree of certainty represent a physical person affiliated with the IIF member organisation. Using CAPTCHAs or relying on an identity proofing process that uses CAPTCHAs (or a technical control of comparable reliability) is a minimally acceptable way of establishing 'humanness' with a sufficient degree of certainty for this assurance profile.

4.3 Credentials Issuance and Technology

- Each subject MUST be represented by an identifier ("username") which MUST be unique for the Identity Provider.
- Subject unique identifiers SHOULD not be re-assigned unless the unique identifier is known to be unused by all relying parties.
- If subjects are allowed access to self-service reset of credentials then either another trusted credential or a one-time password MUST be used.
- Subjects MUST be actively discouraged from sharing credentials with other subjects either by using technical controls or by requiring users to confirm policy forbidding sharing of credentials.
- Measures MUST be taken to reducing the vulnerability of credentials to password guessing attacks.
- Relying Party and Identity Provider credentials (i.e entity keys) MUST NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than a 2048 bit RSA key and MUST be changed at least every 3 years.

4.4 Security and Management of Authentication Events

- Secrets, credentials or long-term keys used in authentication (for instance when authenticating to an Identity Provider) MUST be encrypted if transmitted across open networks (eg. the Internet or Campus networks).
- Any authentication protocols used when authenticating subjects MUST require a proof-of-possession step for subject credentials.
- For regular passwords this involves validating that the user knows her/his password.
- Any session tokens MUST be cryptographically authenticated.
- Authentication mechanisms MUST be protected against common attacks such as man-in-the-middle attacks, eaves-dropper attacks and off-line password guessing.

4.5 Identity Assertion Content

- Each claim MUST contain a permanent identifier of the subject. This identifier MAY be specific to a singly relying party (a so called targeted identifier) or a shared common identifier.
- Each identity claim MUST include a unique representation of the administrative domain associated with the Identity Provider. This identifier MUST NOT be used unless it has been assigned to the Identity Provider by the SWAMID Operations Team.

5 Technical Operational Environment

- The servers and other infrastructure involved in the operation of identity providers or relying parties MUST be maintained according to best practice.

6 Technical representation

For all technology profiles compliance with this identity assurance profile is equivalent with the existence of a valid identity provider issuing valid identity claims.