

# InCommon IAP Support



This document is currently an assessment of the work needed for Registry to support InCommon IAPs out of the box. It is based on v1.1 of the [Identity Assurance Profiles](#). The items described below would be optional, ie: Registry could operate in an IAP compliant manner, but by default would not.

Note that IAP attributes generally apply to Org Identities and not to CO People. As such in a fully federated model, this functionality would not be required.

## For Bronze

1. §4.2.3.2: If a Password Management Plugin is written, it will need to implement character class checks and dictionary checks, or require random passwords.
2. §4.2.5.6: Registry provides support for tracking compliance with acceptable use policies.
3. §4.2.6.1: Registry provides support for provisioning IAQ compliance information to LDAP and/or specified groups.

## For Silver

1. §4.2.2.1: Registry will require Silver IAQ in order to enable COU, CO, or CMP administrative operations.
2. §4.2.2.3.2: OrgIdentity requires additional fields for identity proofing and for date of birth.
3. §4.2.2.3.2: Address types are expanded to include "Address of Record" and "Address of Record (Unconfirmed)".
4. §4.2.2.3.2: Enrollment flows mandate official name per document and address of record.
5. §4.2.2.3.3: OrgIdentity requires status and/or expiration dates.
6. §4.2.2.4.2.2: Enrollment flows collect photo ID information
7. §4.2.2.4.3: Self-Enrollment collects ID number and information and vets against a record checking service (or services)
8. §4.2.2.5: Enrollment flow generates a single use token sent to an email address of record, a token SMS'd to a telephone address of record (for mobile phones), or a letter with a single use token to be printed out and mailed by an admin to a physical address of record. Once the token is provided back, the Address of Record is confirmed.
9. §4.2.2.5: A change in the Address of Record triggers the same confirmation process before the address is considered confirmed.
10. §4.2.3.3: If a Password Management Plugin is written, it will need to implement character class checks and dictionary checks, or require random passwords.
11. §4.2.4.1: Enrollment flows may generate single use tokens where self-enrollment is not in use.
12. §4.2.4.3: If a Password Management Plugin is written, it will need to require an old, unexpired password or the use of pre-registered identity reset questions prior to setting a new password. Registry may track whether a credential is compliant.
13. §4.2.4.4: If a Password Management Plugin is written, it will need to record issuance and revocation events, possibly in Registry's history records.
14. §4.2.5.6: Registry provides support for tracking compliance with acceptable use policies.
15. §4.2.6.1: Registry provides support for provisioning IAQ compliance information to LDAP and/or specified groups.