IGTF Levels of Authentication Assurance

**Version 01-20140908**

**Abstract**

**Identification**

**Table of Contents**

[1 About this document 2](#_Toc397776969)

[2 General Architecture 2](#_Toc397776970)

[3 Identity 2](#_Toc397776971)

[4 Operational Requirements 3](#_Toc397776972)

[5 Site security 3](#_Toc397776973)

[6 Publication and Repository responsibilities 3](#_Toc397776974)

[7 Audits 3](#_Toc397776975)

[8 Privacy and confidentiality 4](#_Toc397776976)

[9 Compromise and disaster recovery 4](#_Toc397776977)

# About this document

*The current version of this document reflects the work of the TAGPMA in extracting the common LoA elements from the SLCS and MICS APs. The text elements have been classified in the AP template format, with the common elements mergen and the differences expressed through selection tables.*

In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119. If a ‘should’ or ‘should not’ is not followed, the reasoning for this exception must be explained to the PMA to make an informed decision about accepting the exception, or the applicant must prove to the PMA that an equivalent or better solution is in place.

# General Architecture

# Identity

## End-entity, subscriber and user identity validation

The initial vetting (proofing?) of identity for any entity in the primary authentication system that is valid for certification should be based on a face-to-face meeting and should be confirmed via photo-identification and/or similar valid official documents. Sufficient information must be recorded and archived such that the association of the entity and the subject DN can be confirmed at a later date. In the case of host or service entities, the initial registration should ensure that the association between the registered owner and the FQDN is correct, and sufficient information should be recorded to contact the registered owner.

In the case where the initial identity vetting is a distributed operation, these rules shall apply for all registration authority (RA) points and all identity validations that result in primary identities. Any distributed RA must have formal authority to recognize and establish end-entity identity.

In all cases, the credentials issued must be bound to the act of identity vetting.

On the Kantara Initiative Identity Assurance Framework Levels of Assurance scale [Kantara2010], Assurance Level 2 and higher are considered sufficient for identity vetting.

## Identifier assignment

The IA assigns unique identifiers to vetted (proofed) entities.

This unique identifier must be linked with one and only one entity for the whole lifetime of the IA service. However, entities may have more than one identifier assigned to them. This identifier may be assigned to a person, a service, or a networked system.

For identifiers assigned to services or networked systems, these identifier will be registered to an owner - being a person or organizational group - that has valid rights to exclusive use of that identifier. Credential issuance will establish the permanent binding between the end-entity, the registered owner, and the identifier, so as to ensure that the name, when subsequently reissued, refers to the same end-entity. This ownership may be re-assigned under controlled circumstances.

For host and service credential requests, the IA or RA should ensure that the requestor is appropriately authorized by the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the credential.

# Operational Requirements

## Communication between Issuing and Registration Authorities

All communications between the Issuing Authority (IA) and the RA regarding credential issuance or changes in the status of a credential must be by secure and auditable methods. The IA must document how changes that may affect the status of the credential are communicated.

## Credentialing process

The association between the act of identity vetting and the issuance of the credential must be secured. The credential must only be issued to the correct entity.

Upon loss of traceability, the IA must suspend or revoke the ability for that individual to obtain a credential and should revoke any already issued credentials.

## Management of assigned credentials

Qualifying IdMs must suspend or revoke authorization to use the service if the traceability to the person is lost. Suspension or revocation must last until identity is updated and confirmed according to IdM policies.

# Site security

# Publication and Repository responsibilities

# Audits

|  |  |  |
| --- | --- | --- |
| ASPEN (‘SLCS’) | BIRCH (‘MICS’) | CEDAR (‘classic’) |
| The IA must verify enough identity information to enable traceback to the physical person at the time of issuance and in keeping with audit retention requirements. | The IA must verify enough identity information to enable traceback to the physical person for at least as long as the credential is valid and in keeping with audit retention requirements.  The IA should verify this information and enable traceback to the physical person for at least one year. | 🡨 *might just be BIRCH* |

Sufficient information must be recorded and archived such that the association of the entity and the subject DN can be confirmed at a later date. In the event that documented traceability is lost, the identifier must never be reissued.

The IA or RA should have documented evidence on retaining the same identity over time.

The IA is responsible for maintaining an archive of these records in an auditable form.

The IA must record and archive all requests for certificates, along with all the issued certificates, all the requests for revocation and the login/logout/reboot of the issuing machine.

The IA must keep these records for at least three years. These records must be made available to external auditors in the course of their work as auditor.

The IA must accept being audited by other accredited CAs to verify its compliance with the rules and procedures specified in its CP/CPS document.

The IA should perform internal operational audits of the IA/RA staff and any underlying systems at least once per year to verify its compliance with the rules and procedures specified in its policies and practices documents. Audit results shall be made available to the accrediting bodies upon request. A list of IA personnel as well as of other personnel critical to the identity vetting process should be maintained and verified at least once per year.

In order to establish the trust of the IA itself, it is recommended that underlying systems make its periodic audits and reviews available to the IA.

In order to establish the trust of the IdM itself, it is recommended that the IA operator request that the IdM system make IdM periodic audits and reviews available.

# Privacy and confidentiality

The Accredited IA must define and follow a privacy and data release policy compliant with the relevant governing legislation. The IA is responsible for recording, at the time of validation, sufficient information to identify the person getting the credential. The IA is not required to release such information unless provided by a valid legal request according to governing laws applicable to that IA.

# Compromise and disaster recovery

The IA must have a business continuity and disaster recovery plan, and be willing to discuss this procedure with the accrediting bodies. The procedure need not be disclosed publicly.

# Other obligations

The IA should make a reasonable effort to make sure that subscribers realize the importance of properly protecting their private data according to the relevant guidelines.

In particular, when using PKI credentials, subscribers should follow the [PKP] guidelines. [needs to be generalised for use with other credentialing systems]

tokens the private key must be protected with a strong pass phrase, i.e., at least 12 characters long and following current best practice in choosing high-quality passwords. Private keys pertaining to host and service certificate may be stored without a passphrase, but must be adequately protected by system methods.

Subscribers must request revocation of any valid credentials as soon as possible, but within one working day after detection of loss or compromise of the credential, or if the data in the credential is no longer valid.