IGTF Levels of Authentication Assurance

**Version 04-20150113**

**Abstract**

**Identification**

urn:oid:…

**Table of Contents**

[1 About this document 2](#_Toc408575894)

[2 General Architecture 2](#_Toc408575895)

[3 Identity 2](#_Toc408575896)

[3.1 End-entity, subscriber and user identity validation 2](#_Toc408575897)

[3.2 Identifier Assignment 3](#_Toc408575898)

[4 Operational Requirements 3](#_Toc408575899)

[4.1 Communication between Issuing and Registration Authorities 3](#_Toc408575900)

[4.2 Credentialing process 3](#_Toc408575901)

[4.3 Management of assigned credentials 3](#_Toc408575902)

[4.4 IT systems security 4](#_Toc408575903)

[4.5 Credential strength 4](#_Toc408575904)

[4.6 Credential validity 4](#_Toc408575905)

[4.7 Identification of credentialing policies 4](#_Toc408575906)

[5 Site security 4](#_Toc408575907)

[6 Publication and Repository responsibilities 4](#_Toc408575908)

[7 Audits 4](#_Toc408575909)

[8 Privacy and confidentiality 5](#_Toc408575910)

[9 Compromise and disaster recovery 5](#_Toc408575911)

[10 Other obligations 5](#_Toc408575912)

# 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

|  |  |  |  |
| --- | --- | --- | --- |
| ASPEN (‘SLCS’) | BIRCH (‘MICS’) | CEDAR (‘classic’) | DOGWOOD (IOTA) |
| Credential life time should be no more than 1Ms | Credential life time should be no more than 400 days if the credential is stored in a file and is further protected with a single authentication factor.  The credential life time MAY be up to 5 times 400 days if the credential is protected with at least two authentication factors none of which is software token. | Credential life time should be no more than 400 days if the credential is stored in a file and is further protected with a single authentication factor.  The credential life time MAY be up to 5 times 400 days if the credential is protected with at least two authentication factors none of which is software token. | The authorities issue long-term credentials to end-entities, who will themselves possess and control their key pair and their activation data.  The subscriber identity is maintained by the credential issuing authority or by third parties trusted by the authority for the purposes of identifier assignment. Any such third parties must have a documented and verifiable relationship with the issuing authority, and through this relationship the issuing authority must have documented, verifiable and auditable means to ensure the requirements of this authentication profile are met. |

To achieve sustainability, it is expected that each IA will be operated as a long-term commitment.

# Identity

## End-entity, subscriber and user identity validation

|  |  |
| --- | --- |
| ASPEN, BIRCH, CEDAR | DOGWOOD |
| On the Kantara Initiative Identity Assurance Framework Levels of Assurance scale [Kantara2010], Assurance Level 2 and higher are considered sufficient for identity vetting. | Any single subject name in a credential must be linked with one and only one entity for the whole lifetime of the service.  Validation of the credential request establishes the permanent binding between the end-entity, the owner, and the subject name. |

|  |  |  |
| --- | --- | --- |
| ASPEN (‘SLCS’) | BIRCH (‘MICS’) | CEDAR (‘classic’) |
| The Site/Organization must provide details of how the site identity management system creates and validates identities for its users.  How it provides DN accountability, showing how they can verify enough identity information to trace back to the physical person for at least one year from the date of certification | [Trusted Agents with a prior documented relationship to be used for attestation of identity. Elaboration of the F2F process or its alternatives needs to be made clear for a generic LoA document. Currently its either real F2F, or video-supported with validated document using notary-public attestations as to authenticity of copy of ID] | [Trusted Agents with a prior documented relationship to be used for attestation of identity. Elaboration of the F2F process or its alternatives needs to be made clear for a generic LoA document. Currently its either real F2F, or video-supported with validated document using notary-public attestations as to authenticity of copy of ID] |

## Identifier Assignment

The name elements contained in the issued credential must be sufficient to uniquely identify an individual.

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.

|  |  |
| --- | --- |
| ASPEN, BIRCH, CEDAR | DOGWOOD |
| 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 - being the responsible administrator or subscriber - 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.  The identifier for human entities should contain an appropriate presentation of the actual name of the entity. | If a name element is included in the credential, it must contain either an opaque unique identifier or a name chosen by the requestor and obtained from (a list proposed by) the identity provider on which the issuer will enforce uniqueness.  The set of name elements included must:   * identify the identity management system via which the identity of this person was vetted, unless the vetting is done directly and solely by the issuing authority; * contain sufficient information such that utilizing only this data, an enquiry  via the issuer to the identity management system or issuing authority allows unique identification of the vetted entity in the identity management system described above;   No anonymous credentials may be issued under this profile. |

# 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.

## Management of assigned credentials

Qualifying IAs 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 IA policies.

|  |  |
| --- | --- |
| BIRCH, CEDAR | ASPEN, DOGWOOD |
| 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. | Upon loss of traceability, the IA must suspend or revoke the ability for that individual to obtain a credential. |

## IT systems security

Systems used by the IA must be located in a secure environment where access is controlled and limited to specific trained personnel.

An IA service systems must be dedicated machines, running no other services than those needed for the IA operations and/or other security-sensitive services. An IA service may be run in a dedicated virtual environment that has the same security for all services running in this environment, it may not leave this security context, and only users who are designated to IA operations may have access to this environment. Any virtualization techniques employed (including the hosting environment) must not degrade the context as compared to any secured physical setup.

## Credential strength

The credential must be tamper proof and not forgeable.

Credentials and credential transport channels over which they are provided must be appropriately protected with a protection strength equivalent to 2048 RSA bit encryption.

## Credential validity

The IA should provide for mechanisms to determine credential validity at the applicable point in time.

## Identification of credentialing policies

The credentialing policies used must be identifiable by relying parties.

# Site security

Mechanisms must be in place to protect the systems and credentials used by the IA. These mechanisms must be well-documented and maintained for the purposes of auditing and accreditation, and the security level should be identifiable by relying parties.

|  |
| --- |
| DOGWOOD (to be discussed for ASPEN, BIRCH) |
| The authority must not knowingly continue to rely on data from third parties that provide inaccurate or fraudulent information. It is strongly recommended that any third party on which the issuing authority relies has an incident response capability and is willing to participate in resolving such incidents. |

# Publication and Repository responsibilities

The IA should publish its policies or independently verified statements of trust regarding its compliance to named policies.

# Audits

|  |  |  |  |
| --- | --- | --- | --- |
| ASPEN (‘SLCS’) | BIRCH (‘MICS’) | CEDAR (‘classic’) | DOGWOOD |
| 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. | 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 must keep these records for at least three years, where the identity validation records must be kept at least as long as there are valid credentials based on such a validation. | At credential issuing time, the authority must reasonably demonstrate how it can verify identity information and trace this information back to a physical person (or for non-human credentials to a named group).  Traceability of the credential is provided only in a cooperative way jointly with other parties that provide other elements of identity-related data. Credentials issued by authorities operating under this Authentication Profile should be used primarily in conjunction with vetting and authentication data collected by the relying parties.  Authorities are not required to collect more data than are necessary for fulfilling the uniqueness requirements. Credentials issued by authorities under this profile may not provide sufficient information to independently trace individual subscribers |

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

|  |
| --- |
| ASPEN, BIRCH, CEDAR |
|  |

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 to verify its compliance with the rules and procedures specified in its policy documents.

|  |  |
| --- | --- |
| ASPEN, BIRCH, CEDAR | DOGWOOD |
|  | At the time of issuance, the authority may rely in good faith on any identity management system by a third party with which it has entered into an agreement and that meets the requirements on third parties set forth in the General Architecture.  The auditing does not necessarily extend to identity vetting systems operated by third parties and used for credential issuance. |

# Privacy and confidentiality

The 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 entity or responsible party to whom the credential is issued. 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 an adequate business continuity and disaster recovery plan, and be willing to discuss this procedure with the relevant 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 credential and the private data contained therein according to the relevant guidelines.

After detection of loss or compromise of a valid credential, subscribers must request revocation of such a credential as soon as possible, at most within one working day. Revocation must also be requested if the data in the credential is no longer valid.

Use of any issued credential implies acceptance by the entity or responsible party of any agreements of the IA pertaining to the issued credential.