Interoperable Global Trust Federation
AP EU TAG

Category:
Status: DRAFT
igtf-authn-assurance-1.5-draft.docx
Editor: Derek Simmel, dsimmel@psc.edu
Last updated: Thu, 03 October 2024
Total number of pages: 8

IGTF Levels of Authentication Assurance

DRAFT Version 1.5-2024

Abstract
The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.
The IGTF Levels of Authentication Assurance (LoA) generalization process aims to extract those elements from 'Authentication Profiles' the IGTF has developed that are of general value to the community. The LoAs described in this document represent the consensus on acceptable levels for the IGTF major relying parties, and are designed such that they also balance the cost and feasibility by the IGTF identity providers.

Identifications
This document: **urn:oid:1.2.840.113612.5.2.6.1.3**
Assurance Level identifications
(*note that no ordering or relative assurance quality must be inferred from identifier assignments)*

ID LoA name	Identifier	*PKI implementation name*
ASPEN	**urn:oid:1.2.840.113612.5.2.5.1**	*SLCS*
BIRCH	**urn:oid:1.2.840.113612.5.2.5.2**	*MICS*
CEDAR	**urn:oid:1.2.840.113612.5.2.5.3**	*Classic*
DOGWOOD	**urn:oid:1.2.840.113612.5.2.5.4**	*IOTA*
ELM	**Urn:oid:1.2.840.113612.5.2.5.5**	*DCVOTA*

Table of Contents

1 About this document 2
1.1 Preamble on assurance equivalence 2
2 General Architecture 2
3 Identity 2
3.1 End-entity, subscriber and user identity validation 2
3.2 Identifier Assignment 4
4 Operational Requirements 5
4.1 Communication between Issuing and Registration Authorities 5
4.2 Credentialing process 5
4.3 Management of assigned credentials 5
4.4 IT systems security 6
4.5 Credential strength 6
4.6 Credential validity 6
4.7 Identification of credentialing policies 7
5 Site security 7
6 Publication and Repository responsibilities 7
7 Audits 7
8 Privacy and confidentiality 8
9 Compromise and disaster recovery 8
10 Other obligations 8

1 About this document

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 relevant accrediting bodies to make an informed decision about accepting the exception, or the applicant must demonstrate to the accrediting bodies that an equivalent or better solution is in place.

To identify the specific Level of Assurance, each has been assigned an opaque name and identifier. Elements of assurance specific to a particular assurance level have been set apart in boxes that are identified by name in each heading indicating the LoA or LoAs to which the elements apply. Text that is not set apart in a particular box is applicable to all assurance levels described.

1.1 Preamble on assurance equivalence

The assurance levels listed are baseline requirements. An actual implementation of any assurance level may exceed the specifications given in this Guideline. Relying parties should exercise their judgement based on the stated assurance level in conjunction with other information and assurances.

Traditionally assurance levels have been identified on a single scale. In terms of a single linear scale, relying parties have often considered authorities compliant with ASPEN, BIRCH, or CEDAR to be similar in terms of assurance level, and authorities compliant with DOGWOOD or ELM to be different. In this document, several aspects are separated and relying parties may find more fine-grained controls.

2 General Architecture

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

3 Identity

3.1 End-entity, subscriber and user identity validation

Credentials issued must be bound to an act of identity vetting.

ASPEN, BIRCH, CEDAR
Sufficient information must be recorded and archived such that the association of the entity and the subject name can be confirmed at a later date. The information collected should be sufficient to trace back to the physical person identified for as long as the credential is valid, but at least one year after credential issuance. 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 authorization of the Issuing Authority to establish end-entity identity. In case of non-personal credential application, the RA should validate the identity and eligibility of the person in charge of the specific entities using a secure method. 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, the registered owner is authorised to request a credential for this entity, and sufficient information should be recorded to contact the registered owner.

ASPEN
The authority must show there is a documented process by which identities are validated and provisioned.

BIRCH, CEDAR
The initial vetting or proofing of identity for any entity in the primary authentication system that is eligible for credential issuance should be based on a face-to-face meeting and should be confirmed via photo-identification and/or similar valid official documents. Identity vetting and validation should be based on • an in-person appearance before a trusted agent of the authority with presentation of a reliable photo-ID and/or valid official documents; or • be validated using notary-public attestations and/or official government data sources and supported by remote live video conversation; or • be performed according to Kantara LoA 2 or better. Identity vetting can also be based on a current and ongoing relationship with the Applicant, that may be verified through the exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds best practice requirements, provided that: (a) identity was originally established with the degree of rigour equivalent to that required above, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret.

CEDAR
The Issuing Authority must keep identity vetting records for at least two years after the last credential issued based on that information is no longer valid.

DOGWOOD
Authorities are only required to collect the data that are necessary for fulfilling the uniqueness requirements. Credentials issued by authorities under this LoA are not required to provide sufficient information to independently trace individual subscribers. 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 LoA should be used primarily in conjunction with vetting and authentication data collected by the relying parties or service providers. Validation of the credential application establishes the permanent binding between the end-entity, the owner, and the subject name. The authority must describe how it can reasonably verify identity information and trace this information back to a physical person (or for non-human credentials to a named group) at the time of credential issuance.

ELM
Authorities are only required to collect the data that are necessary for fulfilling the uniqueness requirements. Credentials issued by authorities under this LoA are not required to provide sufficient information to independently trace individual subscribers. 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 LoA should be used primarily in conjunction with vetting and authentication data collected by the relying parties or service providers. Validation of the credential application establishes the permanent binding between the end-entity, the owner, and the subject name. The authority must describe how it can reasonably verify administrative control of Internet domains in the subject names by the subscriber at the time of credential issuance.

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

3.2 Identifier Assignment

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

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
The identifier for human entities should contain an appropriate presentation of the actual name of the entity. For identifiers assigned to services or networked systems, these identifiers must 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 organisational sub-domain name ownership validation, the domain name registrant must be verified. This verification should be via one of these processes: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; 2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;or 4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN. For host and service credential applications, the IA or RA should ensure that the Applicant 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.

DOGWOOD
The name element in the credential must contain either an opaque unique identifier or a name chosen by the applicant and obtained from (a list proposed by) the identity provider on which the issuer will enforce uniqueness. The set of name elements 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; and • 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 LoA.

ELM
The name elements in the credential must contain FQDNs specified by the applicant and validated by proof of domain administrative control for all corresponding domains, on which the issuer will enforce uniqueness. The set of FQDN name elements must: • each identify the DNS domain via which the FQDN is vetted; and • contain sufficient information such that utilizing only this data, an enquiry by the issuer to the domain management system allows unique identification of the FQDN in the domain management system.

For wildcard certificates, the variable element (*) must precede the domain for which administrative control can be validated. Applications for wildcard certificates must have reasonable scope; for example:

- The wildcard cannot represent a top level domain, such as foo.*bar, foo.co*, nor foo.a*z.
- The wildcard cannot immediately precede a top-level domain, such as *.com, foo*.edu, *bar.org, nor a*z.us.
- For wildcard domains such as *.example.org, foo*.example.org, *bar.example.org, or a*z.example.org, domain administrative control of example.org must be validated.

4 Operational Requirements

4.1 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.

4.2 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.

4.3 Management of assigned credentials

Qualifying IAs must suspend or revoke authorization to use the service if the traceability to the person (ELM: domain administrator) is lost, and such must last until identity (ELM: domain administrator) information is updated or confirmed according to IA policies.

BIRCH, CEDAR
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.

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

ELM
Upon loss of traceability to the domain administrator, the IA must suspend or revoke the ability for the subscriber to obtain a credential. As the administrator of domains for which certificates are issued may change over time, the issuing authority must periodically re-validate control of the domain to sustain validity of issued certificates. Issuing authorities should notify subscribers when changes in domain administration or domain control are observed. If the administrator of domains for issued credentials changes within the validity period of a credential, control of those domains must be re-validated, else the IA must revoke the issued credentials, and suspend or revoke the ability for the subscriber to obtain a credential. Communication means and notification requirements between the IA and subscriber must be specified in the subscriber agreement.

4.4 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.

IA service systems must be dedicated machines, running no other services than those needed for the IA operations and/or equally 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 then must not leave this 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.

4.5 Credential strength

The issued credential must be protected against tampering and not be forgeable.
Credentials and credential transport channels over which they are provided must be appropriately protected with a protection strength equivalent to 112 bits (symmetric)[1].

4.6 Credential validity

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

ASPEN
Credential life time should be no more than 1Ms

BIRCH, CEDAR
Credential life time should be either 1. no more than 400 days if the credential is stored in a file and is further protected with a single authentication factor; or 2. if the credential is protected with at least two authentication factors of which at least one is a hardware token, for no more than 5 times 400 days, during which the credential may be extended or renewed in 400-day increments based on the same data; biometric data need never be changed; or 3. in the case of network and service entities for which the organisational sub-domain name ownership has also been validated, no more than 1200 days, without the possibility for extension or renewal.

DOGWOOD
Credential life time should be no more than 400 days. The subscriber identity is maintained by the 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 assurance level are met.

ELM
Credential life time should be no more than 90 days. The subscriber identity is maintained by the Issuing Authority or by third parties trusted by the authority for the purposes of identifier assignment. Any such third parties (e.g., hosting services) 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 assurance level are met.

[1] To compare implementations, refer to e.g. Special Publication 800-57 Part 1 NIST, 07/2012

4.7 Identification of credentialing policies

The credentialing policies used must be identifiable by relying parties.

5 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, expressed in a way that permits relying parties to assess the assurance provided.

ASPEN, BIRCH, DOGWOOD, ELM
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.

6 Publication and Repository responsibilities

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

7 Audits

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.

The IA must record and archive all requests for credentials, along with all issued credentials, all the requests for revocation and the login, logout, startup, and shutdown 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 accrediting bodies and recognised relying parties to verify its compliance with the rules and procedures specified in its policy documents.

Audit results shall be made available to the accrediting bodies upon request.

ASPEN, BIRCH, CEDAR
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 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. 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 their periodic audits and reviews available to the IA and any accrediting bodies upon request. In order to establish the trust in underlying identity management systems (IdM) itself, it is recommended that the IA operator request that the IdM system make IdM periodic audits and reviews available.

DOGWOOD
The IA should perform internal operational audits of the IA/RA staff at least once per year to verify its compliance with the rules and procedures specified in its policies and practices documents. A list of IA personnel should be maintained and verified at least once per year. At the time of issuance, the authority may rely in good faith on any identity management system of 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.

ELM
The IA should perform internal operational audits of the IA/RA staff at least once per year to verify its compliance with the rules and procedures specified in its policies and practices documents. A list of IA personnel should be maintained and verified at least once per year. At the time of issuance, the authority may rely in good faith on the domain management system of 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 domain management systems operated by third parties and used for credential issuance.

8 Privacy and confidentiality

The IA must publish 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.

9 Compromise and disaster recovery

The IA must have an adequate communications plan and a business continuity and disaster recovery plan, and be willing to discuss these procedures with the relevant bodies. The procedures need not be disclosed publicly.

10 Other obligations

The IA should make a reasonable effort to make sure that credential owners realize the importance of properly protecting their credential and the private data contained therein according to the relevant guidelines.

The IA must inform the credential owner that after detection of loss or compromise of a valid credential, they must request revocation of such a credential as soon as possible, at most within one working day.
Revocation must be requested if the data in a currently valid credential is no longer correct.

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