National Identity Exchange Federation

Trustmark Policy

Version 1.2

August 24, 2021

Table of Contents

1 Introduction and Purpose of This Document

This *Trustmark Policy* governs the lifecycle for trustmarks issued by the National Identity Exchange Federation (NIEF). It covers the topics of trustmark assessment, trustmark issuance, trustmark usage and reliance, trustmark expiration, trustmark revocation, and trustmark reissuance and renewal. It also covers the roles and responsibilities of all parties that enter into legal agreements with NIEF by virtue of having received or relied upon one or more trustmarks issued by NIEF.

1.1 Fundamental Concepts

A *trustmark* is a machine-readable, cryptographically signed digital artifact, issued by a *trustmark provider* to a *trustmark recipient*, and relied upon by one or more *trustmark relying parties*. A trustmark represents an official attestation by the trustmark provider of conformance by the trustmark recipient to a well-defined set of requirements pertaining to trust and/or interoperability for the purpose of interaction with and use of digital information resources and services. A trustmark relying party may rely upon a trustmark as the basis for third-party trust in the trustmark recipient with respect to the set of requirements represented by the trustmark. A *trustmark definition* (TD) expresses the specific set of requirements represented by a trustmark.

A trustmark provider issues, cryptographically signs, and publishes various trustmarks for organizations or business entities (trustmark recipients) that wish to obtain and use those trustmarks as a mechanism for establishing trust with other entities (trustmark relying parties), including partner organizations and individuals. Each of these entities relies on the integrity of the trustmarks issued, which requires implicit reliance on the trustmark lifecycle management process for the trustmarks. For these reasons, NIEF has adopted this Trustmark Policy.

1.1.1 Trustmark Framework Concepts and Definitions

Figure 1 shows the Trustmark Framework Concept Map, which illustrates the basic elements in the *Trustmark Framework*. It indicates at a high level what a trustmark is, how it is defined, and how it is used.

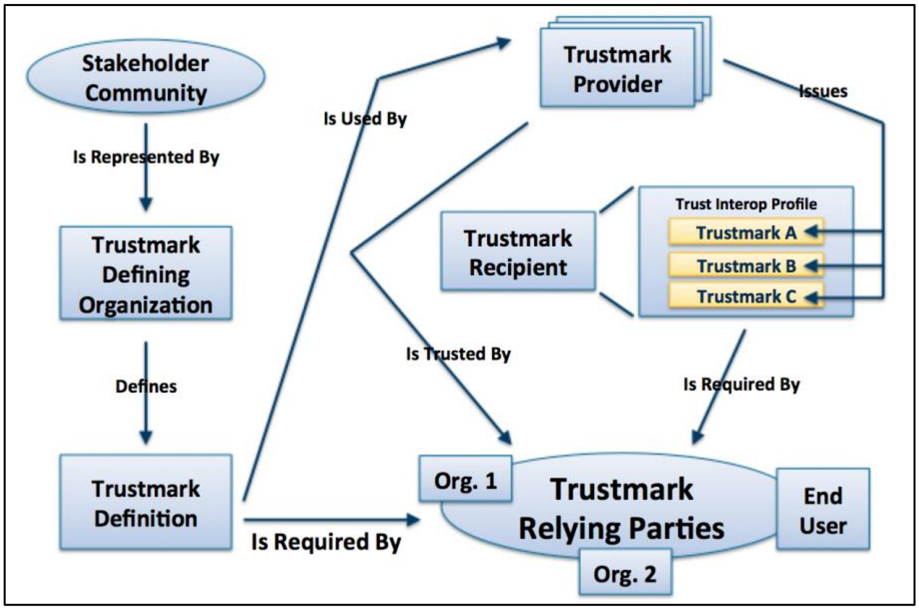

Figure 1: The Trustmark Framework Concept Map

The following terms and concepts are represented in the preceding figure.

A *trustmark* is a machine-readable, cryptographically signed digital artifact that represents a statement of conformance to a well-scoped set of trust and/or interoperability requirements. It exists as an eXtensible Markup Language (XML) object and conforms to a normative specification as defined in [TFTS]. Its issuer, also called the trustmark provider, cryptographically signs it to ensure its integrity.

A *trustmark provider* is an organization or other business entity that issues a trustmark to a *trustmark recipient* based on a formal assessment process. The trustmark serves as a formal attestation by the trustmark provider that the trustmark recipient conforms to a well-defined set of requirements. The trustmark is issued under a *trustmark policy* (not shown in figure) and is subject to a *trustmark recipient agreement* (also not shown in figure). A trustmark recipient is always an organization or other business entity; trustmarks are not issued to individuals.

A *trustmark definition* specifies the *conformance criteria* that the trustmark recipient must meet, as well as the formal assessment process that the trustmark provider must perform to assess whether the trustmark recipient qualifies for the trustmark. There can be many different types of trustmarks, and each type of trustmark has its own trustmark definition.

A trustmark definition is developed and maintained by a *trustmark defining organization*, which represents the interests of one or more stakeholder communities. A trustmark defining organization does not play an active role in the issuance of a trustmark, and does not enter into any legal agreement as part of the issuance or use of trustmarks; its only role is to represent stakeholder communities and publish trustmark definitions that represent the requirements and interests of those communities.

Possession of a trustmark by the trustmark recipient is required by a *trustmark relying party*, which treats the trustmark as 3rd-party-verified evidence that the trustmark recipient satisfies the trust and/or interoperability criteria set forth in the trustmark definition for the trustmark. When it relies on a trustmark, a trustmark relying party enters into a *trustmark relying party agreement* (not shown in figure) with the trustmark provider. A trustmark relying party may be either an organization or an individual.

A *trustmark relying party* defines a *trust interoperability profile* that expresses a trust and interoperability policy in terms of a set of trustmarks that a trustmark recipient must possess, in order to meet its trust and interoperability requirements.

1.1.2 The Trustmark Legal Framework

Figure 2 illustrates the *Trustmark Legal Framework*. It builds upon the basic Trustmark Framework depicted in Figure 1, adding detail about how trustmark issuance, use, and reliance work from a legal perspective.

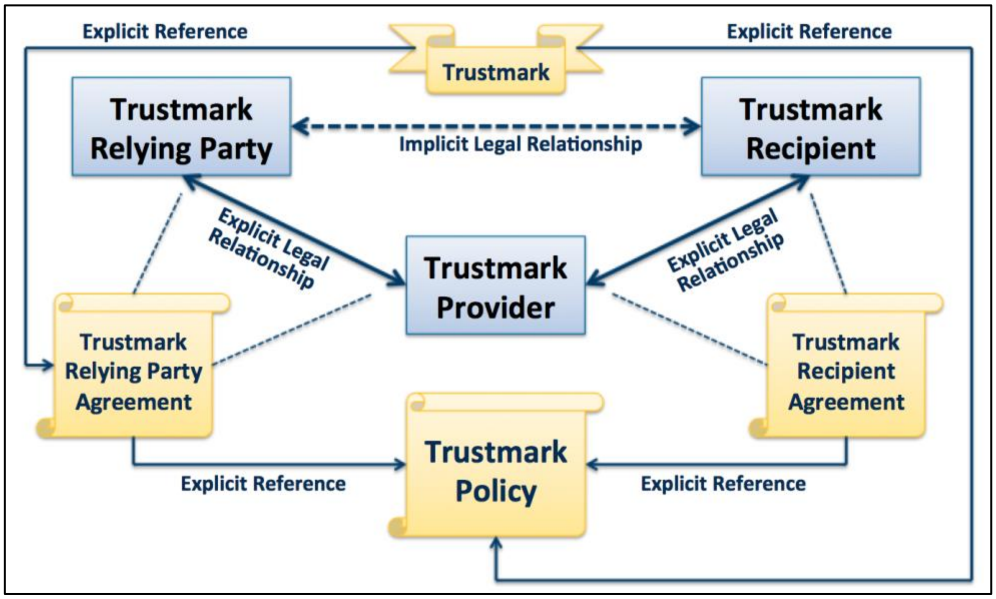

Figure 2: The Trustmark Legal Framework

A trustmark is issued from a trustmark provider to a trustmark recipient under a trustmark recipient agreement, which is a standard two-party contract that establishes an explicit legal agreement between the trustmark provider and trustmark recipient. The trustmark recipient agreement incorporates the trustmark policy by reference. The trustmark provider and the trustmark recipient both must sign the trustmark recipient agreement to execute it.

When a trustmark relying party chooses to rely upon a trustmark, the trustmark relying party must enter into a trustmark relying party agreement with the trustmark provider. The trustmark relying party agreement is also a two-party contract; however, it is not a standard two-party agreement that both parties must sign. Instead, it is a “clickwrap” or “clickthrough” agreement that becomes effective by virtue of the trustmark relying party using or relying on a trustmark issued by the trustmark provider. The trustmark relying party agreement also incorporates the trustmark policy by reference.

Note, as indicated by Figure 2, that the trustmark object contains references to both the trustmark policy under which it was issued and the trustmark relying party agreement to which trustmark relying parties are subject if they choose to use or rely upon the trustmark.

Note also that even though the purpose of a trustmark is to provide a basis for trust between the trustmark recipient and trustmark relying party, the Trustmark Legal Framework does not establish an explicit legal relationship between these two entities. Instead, the framework establishes separate explicit legal relationships between each entity and a third party, the trustmark provider.

1.2 References

Table 1 contains a list of documents that pertain to the contents of this document.

Document ID	Document Name and URL if Applicable
TFTS	Trustmark Framework Technical Specification https://trustmarkinitiative.org/specifications/trustmark-framework/
TSCP	NIEF Trustmark Signing Certificate Policy https://trustmark.nief.org/tat/public/documents/pdf/nief-trustmark-signing-cp-1.3.pdf

Table 1: References for Related Documents

1.3 Document Name and Identification

The name of this document is: “National Identity Exchange Federation Trustmark Policy”.

1.4 Policy Administration

This section includes the name and mailing address of the organization that is responsible for maintaining and updating this document. It also includes the name, email address, and telephone number of a contact person.

1.4.1 Organization Administering the Document

NIEF is the administering organization for this policy. Its full name and mailing address is:

Georgia Tech Applied Research Corporation
National Identity Exchange Federation Center
Georgia Tech Research Institute, Information and Communications Laboratory
75 5th Street, NW

Suite 900
Atlanta, GA 30308

1.4.2 Contact Persons

For executive-level matters, NIEF's Executive Director is:

Mr. John Wandelt
Georgia Tech Research Institute
Information and Communications Laboratory
75 5th Street, NW
Suite 900
Atlanta, GA 30308
Phone: 404-407-8956
Email: John.Wandelt@gtri.gatech.edu

For technical matters related to this policy, NIEF's contact person is:

Mr. Matthew Moyer
Georgia Tech Research Institute
Information and Communications Laboratory
75 5th Street, NW
Suite 900
Atlanta, GA 30308
Phone: 404-407-6679
Email: Matthew.Moyer@gtri.gatech.edu

1.5 Publication of This Document

NIEF maintains this policy at an official, publicly accessible publication location. The publication location of this document is:

https://trustmark.nief.org/tat/public/documents/pdf/nief-trustmark-policy-1.2.pdf

2 Roles and Responsibilities

As introduced previously, there are three primary roles that various entities may play in the issuance and usage of a trustmark. Those roles are:

- The *trustmark provider* (TP), which issues the trustmark;
- The *trustmark recipient* (TR), which is the entity to which and about which the trustmark is issued; and

- The *trustmark relying party* (TRP), which is the entity that uses the trustmark as the basis for making decisions about whether to trust the trustmark recipient.

The following subsections enumerate the responsibilities of each of these roles.

2.1 Trustmark Provider

The trustmark provider is responsible for fulfilling the following obligations under this policy.

1. Establish one or more trustmark provider identifiers (TPIDs) in accordance with the trustmark provider requirements stipulated in [TFTS].

2. Publish one or more trustmark relying party agreements online at well-defined, publicly accessible locations that correspond to the locations cited in trustmarks issued.

3. Perform trustmark assessments for prospective trustmark recipients in accordance with assessment processes as specified in the appropriate trustmark definitions. See Section 3.2 for more information about the trustmark assessment process.

4. Issue trustmarks by generating, cryptographically signing, and publishing them as appropriate for trustmark recipients that meet the required trustmark conformance criteria as specified by the assessment processes in the appropriate trustmark definitions. See Section 3.3 for more information about the trustmark issuance process.

5. Publish a *trustmark status report* (TSR) for each trustmark issued, and update it as required due to trustmark expiration or revocation. See Section 4.3 for more information about how the trustmark provider publishes trustmark status reports for the trustmarks that it issues. Also see Section 4.4 for more information about trustmark expiration, and see Section 4.5 for more information about trustmark revocation.

6. Provide trustmark technical support services to trustmark recipients and trustmark relying parties on a best-effort basis. See Section 5 for more information.

2.2 Trustmark Recipient

By entering into a trustmark recipient agreement with the trustmark provider and receiving one or more trustmarks issued by the trustmark provider, a trustmark recipient is responsible for fulfilling the following obligations under this policy.

1. Cooperate with the trustmark provider as required to establish a trustmark recipient identifier (TRID) (see Section 3.1) and to work through the trustmark application and issuance process (see Section 3.2).

2. Verify the validity of any trustmark issued by the trustmark provider prior to using the trustmark, as per the process described in Section 4.2.1.

3. Use any trustmark issued by the trustmark provider only in accordance with the trustmark's scope of applicability, as described in Section 4.2.2.

4. Promptly report to the trustmark provider any conditions that constitute grounds for revocation of any trustmark issued by the trustmark provider, in accordance with Section 4.5.1.

2.3 Trustmark Relying Party

By using or relying upon any trustmark issued by the trustmark provider, a trustmark relying party automatically enters into a trustmark relying party agreement with the trustmark provider. Under that agreement, the trustmark relying party is responsible for fulfilling the following obligations under this policy.

1. Verify the validity of any trustmark issued by the trustmark provider prior to using or relying upon the trustmark, as per the process described in Section 4.2.1.

2. Use or rely upon any trustmark issued by the trustmark provider only in accordance with the trustmark's scope of applicability, as described in Section 4.2.2.

3 Trustmark Application, Assessment, and Issuance

Organizations that wish to obtain one or more trustmarks from the trustmark provider may do so by completing the steps outlined in the subsections that follow.

3.1 Establishment of a Trustmark Recipient Identifier

As stipulated in [TFTS], before the trustmark provider can issue any trustmarks to a trustmark recipient, the trustmark provider and the trustmark recipient must agree upon a trustmark recipient identifier (TRID) that uniquely identifies the trustmark recipient. The process for establishing a TRID is as follows.

1. The trustmark recipient shall choose its proposed TRID and notify the trustmark provider of its choice. The following rules and guidelines apply to the TRID.

   a. The proposed TRID must be a Uniform Resource Locator (URL) on a Domain Name System (DNS) domain that is under the control of the trustmark recipient.

   b. The proposed TRID should be chosen so as to uniquely identify the trustmark recipient as an organization, even if the organization is a department, subunit, or subsidiary of a larger organization.

      For example, Georgia Tech might choose "https://gatech.edu/" as its proposed TRID. But the Georgia Tech Office of Information Technology, which is a department of Georgia Tech, might choose "https://oit.gatech.edu/" to distinguish itself from its larger parent organization.

   c. A trustmark recipient that plans to obtain trustmarks from multiple trustmark providers should use the same TRID for each trustmark provider. If the trustmark recipient has already established a TRID with one or more other trustmark providers, then it should propose to the trustmark provider the same TRID that it uses for its interactions with one of the other trustmark providers.

   d. A trustmark recipient may use more than one TRID, provided that each TRID is chosen and used in accordance with the guidelines described herein. This practice is recommended in cases where the trustmark recipient wants to assign or apply different trustmarks to different use cases or systems.

2. The trustmark provider shall verify that the trustmark recipient controls the URL proposed as the TRID. The following rules and guidelines apply to the TRID verification process.

   a. The trustmark provider shall verify that the trustmark recipient controls the URL via a simple challenge-response process, in which: (i) the trustmark provider provides a long random number or other hard-to-guess data to the trustmark recipient, (ii) the trustmark recipient publishes the data temporarily at the proposed URL or a sub-path of it, and (iii) the trustmark provider performs a Hypertext Transfer Protocol (HTTP) request of the URL to verify that the trustmark recipient was able to successfully publish the data as required.

   b. The trustmark provider may perform additional steps to verify that the trustmark recipient has positive control of the URL, e.g., verification of DNS domain name registration for the URL via WHOIS lookup, verification of an SSL or TLS certificate for the proposed DNS domain name, etc.

After the TRID establishment process is complete, the trustmark provider shall use the established TRID for all trustmarks that it issues for and about the trustmark recipient.

3.2 Trustmark Application and Assessment Process

At any time after establishing a TRID with the trustmark provider, a trustmark recipient may apply for and undergo assessment for one or more trustmarks.

To apply for a trustmark, a trustmark recipient and the trustmark provider shall follow the process outlined herein.

1. The trustmark recipient shall identify the appropriate trustmark definition describing its desired trustmark. Note that the trustmark provider may not be able to offer certain types of trustmarks, due to trustmark provider restrictions stipulated in the trustmark definition. In addition, the trustmark provider may choose not to offer certain types of trustmarks for business reasons.

2. The trustmark recipient shall notify the trustmark provider of its desire to begin the assessment process for the desired trustmark.

3. The trustmark provider shall assign one or more of its staff members to perform the assessment process for the desired trustmark.

4. The trustmark recipient and trustmark provider assessors shall coordinate as needed to carry out the assessment process for the desired trustmark, taking steps and collecting evidentiary artifacts as stipulated in the appropriate trustmark definition. Note that the assessment process may require the trustmark provider to engage in various activities with third parties to obtain certain information about or on behalf of the trustmark recipient. In such cases, the trustmark provider shall keep the trustmark recipient apprised of any actions involving third parties, as well as the results of those actions.

Note that under some circumstances, it may be logistically preferable for multiple trustmark assessments for the same trustmark recipient to proceed concurrently. The trustmark provider shall make a best effort attempt to perform such assessments concurrently when circumstances permit.

3.2.1 Assessor Qualifications

As stipulated in [TFTS], a trustmark definition may include an “Assessor Qualifications” section that places limitations on who may carry out the trustmark assessment process. In such cases, the trustmark provider shall abide by the specified assessor qualifications and assign only those staff members who meet the specified qualifications to perform assessments for that type of trustmark. If the trustmark provider does not have any staff members who possess the specified qualifications for a trustmark, then the trustmark provider shall not offer that trustmark.

3.2.2 Freshness of Artifacts and Trustmark Period of Validity

As stated in Section 3.3.5, the default period of validity for any trustmark issued by the trustmark provider shall be at most three (3) years; however, the trustmark provider may choose to issue a trustmark with a shorter period of validity if by not doing so, it would cause the trustmark to remain valid after one or more evidentiary artifacts collected during that trustmark's assessment process become too "stale" (i.e., too old) to serve as acceptable evidence in support of the trustmark. In general, the trustmark provider shall not impose any freshness requirements for a trustmark's assessment process artifacts, unless:

1. The trustmark definition for the trustmark explicitly stipulates a freshness requirement, or

2. A particular evidentiary artifact carries an expiration date-time after which it is no longer valid.

3.2.3 Retention of Assessment Process Results and Artifacts

Unless required by law to do otherwise, the trustmark provider shall retain all assessment process results and evidentiary artifacts collected as part of the assessment process for any trustmark requested by a trustmark recipient, regardless of whether the assessment process resulted in issuance of a trustmark. If the assessment process resulted in the issuance of a trustmark, the trustmark provider shall retain assessment process results and evidentiary artifacts collected for a period of at least three (3) years following the expiration of the trustmark. If the assessment process has begun but has not yet been completed and not yet resulted in the issuance of a trustmark, and the trustmark provider has cause to believe that the trustmark recipient is no longer interested in obtaining the trustmark, then the trustmark provider may delete or destroy assessment process results and evidentiary artifacts collected as part of the assessment process at its discretion. In practice, however, the trustmark provider shall make a best-effort attempt to contact the trustmark recipient and verify that it no longer wants to obtain the trustmark prior to deleting or destroying any assessment process results or evidentiary artifacts collected during the assessment process.

3.2.4 Protection and Disclosure of Assessment Process Results and Artifacts

Unless required by law to do otherwise, the trustmark provider shall protect and treat as private and confidential all assessment process results and evidentiary artifacts collected as part of the assessment process for any trustmark requested by a prospective trustmark recipient, and shall not disclose any such information to any third party, regardless of whether the assessment process resulted in issuance of a trustmark.

A trustmark recipient may request a copy of the assessment process results and artifacts collected by the trustmark provider as part of assessment process for any trustmark that it has previously requested, regardless of whether the assessment process resulted in issuance of a trustmark. Any such request must be made in writing. The trustmark provider shall respond to any such request within 60 days.

3.3 Trustmark Issuance

As stipulated in [TFTS], every trustmark definition must specify a formal set of *issuance criteria* that describes what assessment process results are deemed acceptable for trustmark issuance. Following the completion of an assessment for a requested trustmark, if the assessment revealed that the trustmark recipient qualifies for issuance of the trustmark as per the issuance criteria specified in the appropriate trustmark definition, the trustmark provider shall issue the trustmark within three (3) business days, or within a time period that is mutually agreed upon by the trustmark provider and the trustmark recipient. The following subsections describe specific aspects of the trustmark issuance process.

3.3.1 Signing of Trustmarks and Protection of Trustmark Signing Certificates

Each trustmark issued by the trustmark provider shall be digitally signed with a *trustmark signing certificate*, to cryptographically ensure its integrity for the benefit of the trustmark recipient and all trustmark relying parties who may rely on the trustmark. To establish and maintain a high degree of confidence in digital signatures on the trustmarks that it issues, NIEF has established a *National Identity Exchange Federation Trustmark Signing Certificate Policy* that governs the management of all trustmark signing certificates maintained and used by NIEF. The NIEF Trustmark Signing Certificate Policy is available at the following location.

https://trustmark.nief.org/tat/public/documents/pdf/nief-trustmark-signing-cp-1.3.pdf

3.3.2 Conformance of Trustmarks to Trustmark Framework Specifications

All trustmarks issued by the trustmark provider shall conform to the normative technical specification for trustmarks as described in [TFTS].

3.3.3 Use of Identifiers in Trustmarks Issued

As stipulated in [TFTS], all trustmarks must contain the following identifiers:

1. A trustmark provider identifier (TPID) that uniquely identifies the trustmark provider;

2. A trustmark recipient identifier (TRID) that uniquely identifies the trustmark recipient;

3. A trustmark identifier that uniquely identifies the trustmark.

As noted in Section 2.1, a trustmark provider must establish one or more TPIDs. As per [TFTS], each TPID established by a trustmark provider must be a URL that is owned or controlled by the trustmark provider. Each trustmark issued by the trustmark provider shall contain one of the trustmark provider's TPIDs, thereby identifying the trustmark provider as the trustmark issuer.

In addition, each trustmark issued by the trustmark provider shall contain the TRID that was established between the trustmark provider and the trustmark recipient prior to trustmark issuance via the process specified in Section 3.1.

Finally, each trustmark issued by the trustmark provider shall contain a trustmark identifier that is a sub-path of one of the trustmark provider's TPIDs. If any trustmark claims to be issued by the trustmark provider, but its identifier is not a sub-path of one of the trustmark provider's TPIDs, then the trustmark is invalid, and trustmark recipients must not use it and trustmark relying parties must not use it or rely upon it.

3.3.4 Publication of Trustmarks Issued

Each trustmark issued by the trustmark provider shall be published online at a publicly accessible URL that matches the trustmark's identifier, unless the trustmark recipient requests that the trustmark not be published online; however, trustmark recipients are strongly encouraged to permit the trustmark provider to publish their trustmarks online, as failing to publish a trustmark at a publicly accessible URL that matches its identifier can lead to numerous practical challenges for trustmark relying parties that may attempt to rely on the trustmark.

3.3.5 Period of Validity for Trustmarks Issued

By default, every trustmark issued by the trustmark provider shall expire after a period of three (3) years, unless the TD for that trustmark recommends or mandates an alternate period of validity, in which case the trustmark provider shall comply with the TD's recommendation or mandate as appropriate, or unless the trustmark provider chooses to specify a shorter period of validity due to concerns about assessment process artifact freshness as specified in Section 3.2.2. A trustmark recipient wishing to obtain a trustmark with a non-standard period of validity may do so by written request to the trustmark provider prior to the issuance of the trustmark. The trustmark provider reserves the right to deny any such request or choose a different period of validity if the requested alternate period of validity is deemed to be unacceptable for any reason.

3.3.6 Issuance of Provisional Trustmarks with Documented Exceptions

In some cases, and for various reasons, it may be desirable for a prospective trustmark recipient to receive a trustmark without meeting all of the requirements for issuance of the trustmark as per the issuance criteria specified in the appropriate trustmark definition. To accommodate such cases, the trustmark provider shall maintain the capability to issue a *provisional trustmark* to a trustmark recipient when circumstances warrant it. Issuance of provisional trustmarks by the trustmark provider shall be subject to the following rules.

1. The trustmark provider shall issue a provisional trustmark only under circumstances in which the assessment process indicates that the prospective trustmark recipient (a) meets the majority of the conformance criteria as specified in the appropriate trustmark definition, and (b) complies with the overall spirit and intent of the trustmark definition despite not explicitly fulfilling the conformance criteria, as judged by the assessor who carried out the assessment process.

2. Each provisional trustmark issued by the trustmark provider shall contain the following supplemental information: (a) a Boolean indicator denoting that assessment exceptions have been granted to the trustmark recipient, and (b) a brief description of each assessment exception granted. This information shall appear within the "Provider Extensions" element of the provisional trustmark, and shall be encoded in a format that permits straightforward machine processing of the aforementioned Boolean indicator.

3. Prior to publishing the provisional trustmark with the aforementioned supplemental information, the trustmark provider shall secure written permission from the prospective trustmark recipient to include this information in the trustmark. If the prospective trustmark recipient refuses to allow the inclusion of this supplemental information within the provisional trustmark, then the trustmark provider shall not issue the provisional trustmark.

4. Each provisional trustmark issued by the trustmark provider shall carry a period of validity no greater than six (6) months.

4 The Trustmark Lifecycle

As specified in [TFTS], after a trustmark has been issued, it always exists in one of three states throughout its lifecycle. Those states are:

1. "ACTIVE",

2. "EXPIRED", and

3. "REVOKED".

Logically, if a trustmark has been issued, has not yet expired, and has not yet been revoked, then it is active. Once it has expired or been revoked, a trustmark can never return to an active state.

The following subsections discuss the various states of the trustmark lifecycle.

4.1 Trustmark Issuance

[TFTS] specifies a set of trustmark issuance prerequisites and requirements. The trustmark provider shall comply with all such trustmark issuance prerequisites, and all trustmarks issued by the trustmark provider shall conform to the trustmark issuance requirements. See Section 3.3 for information about the trustmark issuance process.

4.2 Trustmark Usage and Terms of Acceptable Use

Prior to using or relying upon a trustmark issued by the trustmark provider, both the trustmark recipient and the trustmark relying party must perform a series of operations to ensure that the trustmark is valid and that the intended usage of it or reliance upon it falls within the trustmark's Scope of Applicability. Sections 4.2.1 and 4.2.2 address each of these topics in turn. Section 4.2.3 addresses the more advanced topic of binding trustmarks to system endpoints.

4.2.1 Trustmark Validity

Verification of the validity of a trustmark issued by the trustmark provider requires the following steps.

1. *Verification of the Trustmark's Digital Signature*: Verify that the digital signature on the trustmark is cryptographically consistent with the trustmark's contents.

2. *Verification of the Trustmark Signing Certificate's Common Name*: Verify that the trustmark signing certificate used to sign the trustmark contains the appropriate common name, as specified in [TSCP].

3. *Verification of the Trustmark Signing Certificate's Status*: Verify that the trustmark signing certificate used to sign the trustmark has not expired or been revoked.

4. *Verification of the Trustmark Provider Identifier*: Verify that the trustmark provider identifier (TPID) on the trustmark is consistent with one of the trustmark provider's TPIDs.

5. *Verification of the Trustmark's Identifier*: Verify that the trustmark's identifier is a sub-path of one of the trustmark provider's TPIDs. Note that both a TPID and a trustmark identifier must always be a valid URL.

6. *Verification of Trustmark Non-Expiration*: Verify, via the expiration date-time on the trustmark, that the trustmark is not yet expired.

7. *Verification of Trustmark Non-Revocation*: Verify, through the trustmark status report at the trustmark's status URL, that the trustmark has not been revoked. Section 4.3 contains more information about trustmark status checking.

If any of the above verification steps results in failure, then the trustmark is invalid. A trustmark recipient must not use an invalid trustmark or make any representations indicating that the trustmark is valid. Also, a trustmark relying party must not use or rely upon an invalid trustmark as the basis for making trust or interoperability decisions. Both the trustmark recipient and the trustmark relying party shall bear any and all losses or legal consequences that may arise due to their failure to comply with these requirements.

4.2.2 Scope of Trustmark Applicability

In addition to verifying a trustmark's validity, entities that use or rely upon a trustmark issued by the trustmark provider must respect the trustmark's scope of applicability, as follows.

1. *Verification of Proper Organizational Scope via the Trustmark Recipient Identifier*: Verify that the trustmark recipient identifier (TRID) matches and/or logically corresponds to a known URL for the entity about which the trustmark was (or is assumed to have been) issued, and for which the trustmark conveys trust. For example, when choosing whether to trust an entity associated with the URL http://example.com/, or services offered at endpoints at sub-paths or sub-domains of example.com, the entity making the trust decision should verify that all trustmarks to be relied upon contain a TRID of http://example.com/ or something similar, e.g., an appropriate subdomain of http://example.com/.

2. *Verification of Proper Operational Scope via the Trustmark Definition*: Verify that the purpose for which the trustmark will be used, or the purpose for which it will be relied upon, is consistent with the trustmark's meaning and intended usage as per its trustmark definition.

If any of the above verification steps results in failure, then the intended usage of the trustmark is outside its scope of applicability. A trustmark recipient must not use a trustmark, and a trustmark relying party must not use or rely upon a trustmark, except in accordance with the trustmark's scope of applicability. Both the trustmark recipient and the trustmark relying party shall bear any and all losses or legal consequences that may arise due to their failure to comply with these requirements.

4.2.3 Binding of Trustmarks to Operational System Endpoints

While it is possible to use and rely upon a trustmark in a variety of ways, one common way to use a trustmark is to bind it to one or more system endpoints operated by the trustmark recipient. Binding of trustmarks to system endpoints may be performed by various types of entities, including the trustmark recipient itself, a federation operator, or a registry operator. The binding of trustmarks to a system endpoint enables users of the endpoint to make trust and interoperability decisions about the endpoint based on the trustmarks bound to it. Accordingly, the trustmark provider permits the trustmarks that it issues to be bound to system endpoints, under the following conditions.

1. The binding must fall within the trustmark's scope of applicability (see Section 4.2.2).

2. Any entity that binds a trustmark to a system endpoint shall be considered a trustmark relying party, and is subject to the trustmark relying party agreement associated with the trustmark for the duration of the trustmark's binding to the system endpoint.

3. If an entity chooses to rely upon a trustmark for the purpose of making trust or interoperability decisions about a system endpoint to which the trustmark is bound, then in addition to acting as a trustmark relying party for the trustmark, that entity is also responsible for performing any necessary due diligence to confirm that the binding of the trustmark to the system endpoint falls within the trustmark's scope of applicability.

4.3 Trustmark Status Checking

In accordance with [TFTS], for each trustmark that it issues, the trustmark provider shall publish a trustmark status report at a publicly accessible URL that matches the status URL field in the trustmark. The trustmark status report shall indicate whether the trustmark is still active, expired, or revoked.

The status URL for all trustmarks issued by the trustmark provider shall be a sub-path of one of the trustmark provider's TPIDs. If any trustmark claims to be issued by the trustmark provider, but its status URL is not a sub-path of one of the trustmark provider's TPIDs, then the trustmark is invalid, and trustmark relying parties must not use it or rely upon it.

If a trustmark expires or becomes revoked, and another trustmark or set of trustmarks has been issued by the trustmark provider to supersede the expired or revoked trustmark, the trustmark status report for the expired or revoked trustmark shall indicate the superseding trustmark(s) via the one or more "Superseder" fields, in accordance with [TFTS]. Indication of superseding trustmarks can be useful for continuity of trustmark-based trust in cases where a trustmark relying party was not previously aware of a change in the status of a trustmark, e.g., if a trustmark has been revoked and subsequently replaced with a new trustmark that conveys the same meaning as the revoked trustmark.

A trustmark relying party for the trustmark may query the trustmark's status URL as needed to check whether the trustmark's status has changed. When querying the trustmark's status URL, a trustmark relying party should verify that the TLS certificate used to protect the status

URL is valid and not revoked.[1] The trustmark provider shall use only TLS certificates issued by certificate authorities that appear in popular web browsers, or certificate authorities that have a chain of trust to other certificate authorities that appear in popular web browsers. trustmark relying parties can therefore perform TLS certificate verification using standard Public Key Infrastructure (PKI) trust chain verification techniques.

4.4 Trustmark Expiration

In accordance with [TFTS], every trustmark issued by the trustmark provider shall specify its expiration date-time. A trustmark expires immediately when its expiration date-time has passed. After the trustmark has expired, the trustmark provider shall no longer uphold or stand by any promises, representations, or warranties made in connection with the issuance of the trustmark.

4.5 Trustmark Revocation

By revoking a trustmark, the trustmark provider is effectively indicating to the trustmark recipient and all trustmark relying parties that the trustmark is no longer valid for some reason. The following subsections describe how trustmark revocation works for trustmarks issued by the trustmark provider.

4.5.1 Conditions for Revocation

As specified in [TFTS], if at any time following the issuance of a trustmark and prior to the trustmark's expiration, the trustmark recipient no longer complies with one or more of the conformance criteria specified for the trustmark by its trustmark definition, then the trustmark shall be immediately considered invalid and must be revoked. The trustmark recipient must notify the trustmark provider immediately upon learning of any conditions that invalidate the trustmark. In the event that the trustmark recipient fails to immediately notify the trustmark provider of any such condition, the trustmark recipient shall bear the legal consequences of this failure.

In addition, if at any time following the issuance of a trustmark and prior to the trustmark's expiration, any of the trustmark's *trustmark revocation criteria* are met, the trustmark shall be immediately considered invalid and must be revoked. The trustmark revocation criteria are an optional component of a trustmark definition, as specified in [TFTS]. The trustmark recipient must notify the trustmark provider immediately upon learning that any trustmark revocation criteria have been met. In the event that the trustmark recipient fails to immediately notify the trustmark provider of any such condition, the trustmark recipient shall bear the legal consequences of this failure.

[1] TLS certificate status checking is recommended for additional security, because as per [TFTS], a trustmark provider is not required to attach a digital signature to a trustmark status report.

Finally, if at any time following the issuance of a trustmark and prior to the trustmark's expiration, the trustmark recipient agreement between the trustmark provider and the trustmark recipient becomes void for any reason, then the trustmark shall be immediately considered invalid and must be revoked.

In the event of a trustmark revocation, the trustmark recipient may seek issuance of a new trustmark in place of the revoked trustmark by first remedying the violated conformance criteria, and then undergoing a new assessment process as specified in Section 4.6.

4.5.2 Revocation Process

Upon learning that a trustmark has become invalid, the trustmark provider shall revoke the trustmark within 24 hours. The trustmark provider shall perform the revocation by updating the trustmark status report for the revoked trustmark as appropriate to indicate that the trustmark has been revoked.

4.5.3 Notification of Revocation to Trustmark Relying Parties

Upon revocation of a trustmark by the trustmark provider, the trustmark recipient must immediately discontinue the use of the trustmark. In addition, the trustmark recipient should immediately notify any trustmark relying party that relies upon the revoked trustmark, and the trustmark recipient must make a best-effort attempt to avoid engaging in any business transactions with a trustmark relying party that is relying upon the revoked trustmark.

The trustmark provider is not responsible for any damages that may result from the use or reliance upon a revoked trustmark. Also, because the trustmark provider cannot know with certainty all trustmark relying parties for a trustmark that it issues, the trustmark provider is not responsible for notifying trustmark relying parties of a trustmark revocation event, other than via the revocation process described in Section 4.5.2.

4.6 Trustmark Renewal and Reissuance

The trustmark lifecycle process does not permit for the renewal or reissuance of trustmarks that have expired or been revoked. A trustmark recipient may seek issuance of a new trustmark in place of an expired or revoked trustmark; however, issuance of a new trustmark requires a new assessment as per the assessment process specified in the appropriate trustmark definition. Note that, if not explicitly prohibited under the appropriate trustmark definition and if deemed appropriate by the trustmark provider, the trustmark provider may leverage artifacts collected during a prior trustmark assessment when performing a new assessment for the same type of trustmark.

5 Trustmark Technical Support Services

The trustmark provider shall provide at least a minimum level of basic, best-effort technical support to trustmark recipient and trustmark relying parties that want to use or rely upon the trustmarks that it has issued.