Trademark Clearinghouse:
Draft Implementation Model

ICANN

13 April 2012

Contents

EXECUTIVE SUMMARY ... 3

Part 1 – Introduction and Background ... 7

1.1 About this Document ... 7

1.2 About the Implementation Assistance Group ... 7

1.3 Terminology ... 7

Part 2 – Authentication and Validation Processes ... 9

2.1 Authentication of Trademark Data ... 9

2.2 Validation for Proof of Use ... 14

2.3 Updates and Renewals of Clearinghouse Records ... 17

2.4 Removal of Clearinghouse Records ... 18

2.5 Audit and Logging Requirements ... 19

Part 3 – Sunrise and Trademark Claims Processes ... 20

3.1 Sunrise ... 20

3.2 Trademark Claims ... 23

3.3 Audit and Logging Requirements ... 26

3.4 Communications Protocols ... 27

3.5 Data Locations and Data Access ... 33

3.6 Extending Mandatory Rights Protection Mechanisms ... 39

Part 4 – Dispute Resolution ... 41

4.1 Disputes concerning Clearinghouse Processes ... 41

4.2 Sunrise Disputes ... 42

4.3 Trademark Claims disputes ... 43

Part 5 – Additional Considerations ... 45

5.1 Note on Ancillary Services ... 45

5.2 Matching Rules ... 45

5.3 Costs ... 46

EXECUTIVE SUMMARY

The Trademark Clearinghouse ("Clearinghouse") facilitates the protection of trademark rights during the initial allocation and registration periods for domain names in new generic top level domains (new gTLDs). Starting with the first round expected to be coming online early in 2013, all new gTLD registries will be required to use Clearinghouse data to ensure that a set of mandatory trademark rights protection mechanisms are applied to all new domain registrations occurring in at least the first 90 days of domain registration.

The Clearinghouse collects information about trademark rights directly from the holders and representatives of such rights, and communicates that information with registry operators, so that the registries can:

- offer Sunrise registration services which provide rights holders the opportunity to register domain names in a TLD before registration is generally available to the public, and
- provide notification to and require acknowledgement from a prospective registrant that a domain name matches a Clearinghouse record. This permits a potential registrant to assess the risks of registering a given domain name, and is intended to help reduce infringement of trademark rights in the DNS.

The Clearinghouse will promptly notify participating rights holders when domain names matching Clearinghouse records are registered during a TLD's startup periods.

The Clearinghouse model has been structured to streamline the domain registration process for rights holders and for gTLD registries, while ensuring that an adequate level of protection is in place to reduce the occurrence of rights infringement in the domain name market. At the same time, it closely authenticates and validates rights assertions to ensure that legal rights are protected without expanding those rights unfairly at the expense of legitimate fair use or free expression.

The Clearinghouse model has undergone extensive review and design work to ensure that proper safeguards are in place to prevent misuse of trademark data. It is structured to ensure integrity, timeliness, and efficiency within the domain registration process.

FOCUSED ROLE FOR THE CLEARINGHOUSE

The Clearinghouse will play the role of information warehouse—collecting, authenticating, storing, and distributing the information it receives in a secure and efficient manner. Standards ensuring that the Clearinghouse is in the role of "fact verifier" will be in place, limiting the discretion that can occur in any result, and creating consistency across the process. Processes will ensure that that every decision made by the Clearinghouse can be reproduced if re-examined at a later date. Logging and audit trails will ensure that such re-examination can occur if required.

CLEAR COMMUNICATION AND RESPONSIBILITY

The Clearinghouse will communicate directly with rights holders to receive rights information (including requests to update and maintain trademark data when required), and to provide required notifications about domain name activity. In addition, it will communicate directly with registries to ensure that current rights data is available for registry services. Registrars will communicate with domain name registrants and with registries, in keeping with their current registration practices.

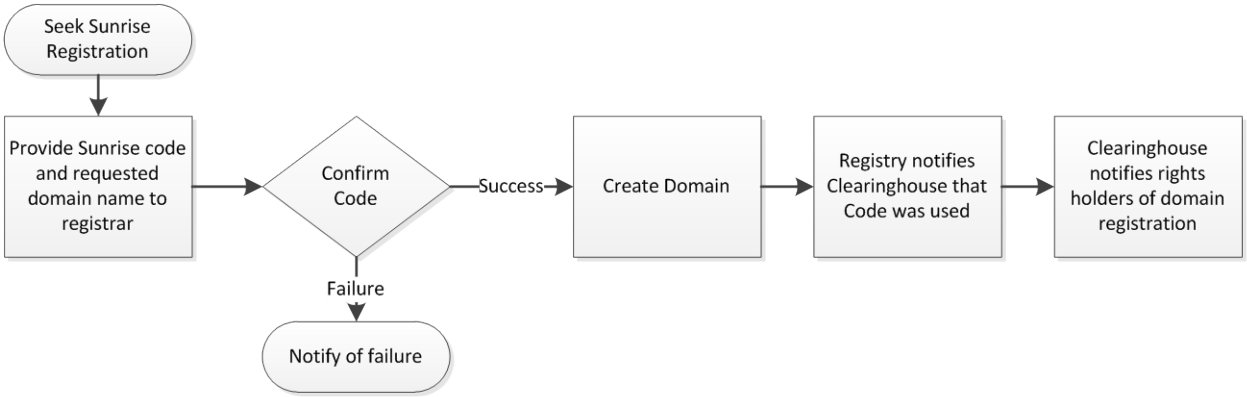
STRUCTURAL DATA PROTECTIONS FOR CONFIDENTIALITY AND INTEGRITY

Beyond the contractual controls anticipated to be applicable to use of data, the Clearinghouse model also includes cryptographic protection of the data it distributes, to ensure that information deemed sensitive is protected against misuse and abuse. Through the use of established and well-understood one-way encryption algorithms (HMAC-SHA1), matching processes can occur without exposing any potentially sensitive data. This permits the Clearinghouse to provide data sets to registries that facilitate the necessary lookup functions for rights protection mechanisms without exposing any trademark data. Where more than a simple match function is required, the Clearinghouse uses an encryption structure built on AES256 that ensures that all and only the necessary data is available.

SUNRISE BASED ON CODES GIVEN TO MARK HOLDERS

Rights holders obtain validation that their marks meet mandatory Sunrise eligibility requirements from the Clearinghouse and are given a Sunrise validation code. Codes are specific to the receiving registry and are single-use to deter fraud and abuse.

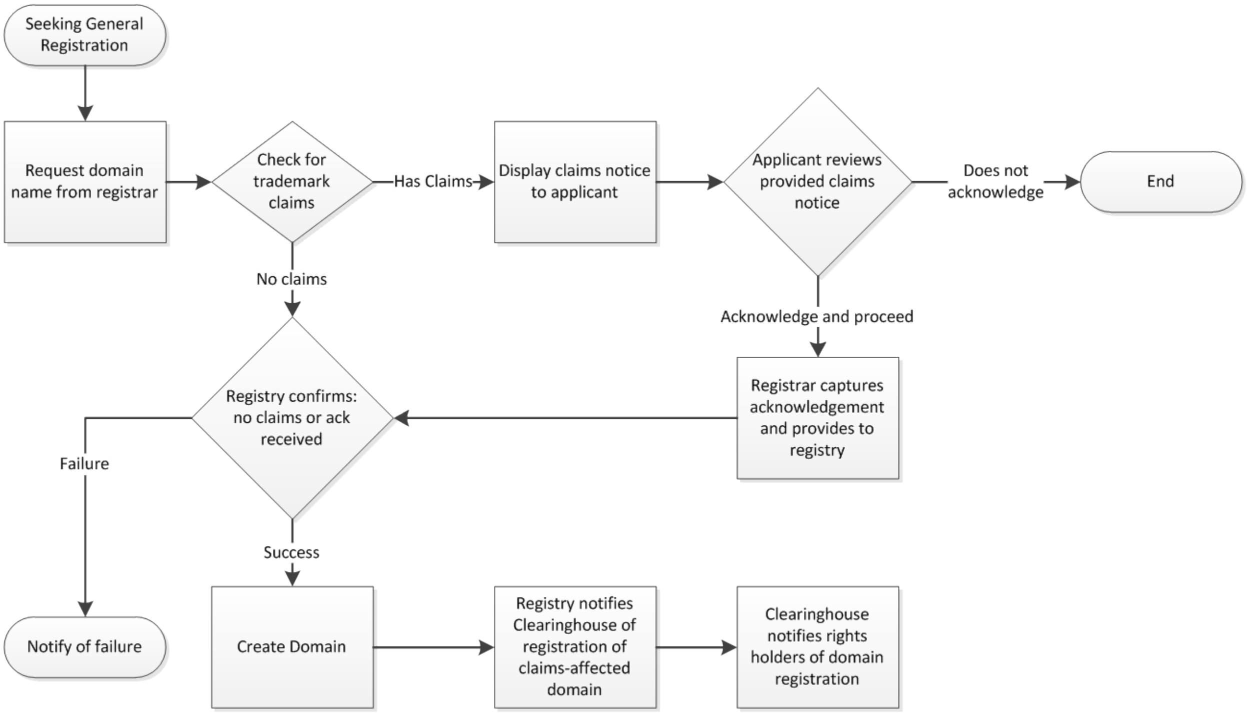
A simplified version of the sunrise process follows:


Seek Sunrise Registration
Provide Sunrise code and requested domain name to registrar
Confirm Code
Success
Create Domain
Registry notifies Clearinghouse that Code was used
Clearinghouse notifies rights holders of domain registration
Failure
Notify of failure

TRADEMARK CLAIMS BASED ON UPDATED FILES

Registries will process Trademark Claims based on a file provided by the Clearinghouse, that is updated/refreshed at regular intervals. This provides reliability and responsiveness to support the introduction of this step into the registration process with minimal changes needed.

A simplified version of the Trademark Claims process follows:


Seeking General Registration
Request domain name from registrar
Check for trademark claims
Has Claims
Display claims notice to applicant
Applicant reviews provided claims notice
Does not acknowledge
End
No claims
Acknowledge and proceed
Registrar captures acknowledgement and provides to registry
Registry confirms: no claims or ack received
Failure
Success
Notify of failure
Create Domain
Registry notifies Clearinghouse of registration of claims-affected domain
Clearinghouse notifies rights holders of domain registration

IDN READY

The Clearinghouse will accept trademark information in its native form (i.e., using the Unicode character set); specific variant character mappings must be handled by the registry.

ADAPTATION TO INDIVIDUAL REGISTRY MODELS

By storing encrypted data at each participating registry, the Clearinghouse assures that registries are enabled to meet their contractual obligation to provide rights protection mechanisms during the launch phase of each new gTLD, without forcing a registry to choose any given set of business rules or Sunrise processes. Extensions to the Extensible Provisioning Protocol (EPP) for communication between registries and registrars are backward compatible (i.e., work with existing versions), but support rights protection during the mandatory periods. Local storage isolates and simplifies Clearinghouse technical functionality, ensuring that each unique registry can choose the best way to implement and deliver registration services for its specific business needs.

Part 1 – Introduction and Background

1.1 About this Document

This document provides a draft implementation model for the Trademark Clearinghouse and its associated processes. This model is subject to change based on additional feedback, provider requirements, or other considerations, and is expected to continue to develop over time.

1.2 About the Implementation Assistance Group

This model reflects the input of the Implementation Assistance Group (IAG) participants and is being circulated for review and comment by this group. The IAG was convened on the basis of an open call for volunteers[1] and considered a set of implementation issues relating to the Trademark Clearinghouse. The IAG discussions took place from November 2011 through March 2012, via written submission of comments and a series of conference calls on a time zone-rotated basis. Two parallel tracks focused on process requirements and on technical issues, respectively.

The purpose of the IAG was to provide advice on key Clearinghouse processes and technical implementation issues. The goal set was to deliver a set of high-level business requirements to the Service Provider(s) selected out of the RFI process.[2] The IAG was not tasked with designing complete solutions for implementation.

The proceedings of the group, including statements of interest, issue papers, conference call recordings, and mailing list archives, are available at https://community.icann.org/display/cctrdmrkclrnghsiag/Home.

1.3 Terminology

This section provides a review of terminology used in the document. A complete set of standard terms and definitions will continue to be established, but a brief list is included below to provide guidance on the terms used in this document.

[1] http://www.icann.org/en/news/announcements/announcement-26oct11-en.htm

[2] http://www.icann.org/en/news/announcements/announcement-5-03oct11-en.htm

Ancillary service: A service that is not required, but is optionally offered by the Clearinghouse or by others.

Authentication: Establishing that trademark and contact information is true, accurate and meets all criteria for Clearinghouse inclusion. All Clearinghouse records will be authenticated.

Clearinghouse provider: An entity designated to perform one or more of the Clearinghouse functions.

Clearinghouse record: Rights data submitted to the Clearinghouse pertaining to a particular mark.

Domain name applicant: An entity initiating registration of a domain name.

Identical match: A correspondence between the textual elements of a mark and a given domain name, based on a defined set of rules.

Label: A potentially valid DNS label (domain name) generated from a Clearinghouse record using the "identical match" rules.

Prospective registrant: See "domain name applicant."

Rights holder: The person or entity holding a set of rights pertaining to a particular mark.

Sunrise Code: A code generated by the Clearinghouse to indicate that a Clearinghouse record meets minimum Sunrise eligibility requirements.

Trademark string: A word mark exactly as it is registered with the appropriate jurisdictional trademark authority or is protected by statute, treaty, or validated by court proceeding.

Validation: Establishing that an authenticated trademark record meets the Clearinghouse standard for Sunrise eligibility, including demonstration of use of the trademark.

Part 2 – Authentication and Validation Processes

This section describes processes for entering rights data into the Clearinghouse database (i.e., creating Clearinghouse records). Recording trademark data in the Clearinghouse is voluntarily undertaken by a rights holder. For inclusion in the Clearinghouse, a mark should be:

a. a nationally or regionally (i.e., multi-nationally) registered word mark from any jurisdiction;

b. a word mark that has been validated through a court of law or other judicial proceeding;

c. a word mark protected by a statute or treaty in effect at the time the mark is submitted to the Clearinghouse for inclusion; or

d. another mark that constitutes intellectual property.

2.1 Authentication of Trademark Data

The Trademark Clearinghouse is a central repository for information to be authenticated, stored, and disseminated, pertaining to the rights of trademark holders. One of the core functions of the Clearinghouse will be authentication of the data to be included. A clear set of authentication standards must be adopted and published prior to the submission of any data by rights holders. This will also serve the goals of an efficient, predictable process.

In addition, a key requirement is for the Clearinghouse to serve rights holders from all regions of the world. The processes and requirements for recording rights data in the Clearinghouse must be accessible to and communicated to prospective users in all regions.

An online submission process is recommended for input of data to the Clearinghouse. Physical copies of trademark registration data should not generally be required, but may be accepted by the Clearinghouse where necessary.

Recommended requirements are described in this section.

2.1.1 Clearinghouse Role in Authentication

To facilitate prompt authentication reviews, all determinations should be made on the basis of a programmatic review of the data submitted, rather than on extended dialogues between submitters and the Clearinghouse. If data is not capable of authentication as submitted, it should generally be rejected without any prejudice toward resubmission of the data. However, some description as to the basis for the deficiency should be provided in every case so that the deficiency can be corrected.

The Clearinghouse will not perform an in-depth review of the basis for the rights being claimed. This was considered in terms of a cost-benefit analysis, with the expectation that a focused role for the Clearinghouse leads to greater efficiencies and lower cost. The capability for the Clearinghouse to apply legal analysis and adjudicate issues concerning legal rights might be a useful secondary service in some cases; however, this is considered outside the scope of the core function of the Clearinghouse.

2.1.2 Name of Rights Holder and Submitting Party

The authentication process should ensure a correspondence between the trademark holder noted in the relevant jurisdiction, and the name of the holder listed for the Clearinghouse record. Where the name submitted to the Clearinghouse matches the name associated with the registration of the trademark in the issuing jurisdiction, verification of the rights holder can be a simple and straightforward process.

In the case where the names do not match, evidence such as assignment documentation will need to accompany the submission. The objective is to ensure that the entity asserting the rights is authorized by the rights holder to exercise those rights. These cases will require specific review steps by the Clearinghouse to authenticate the supporting documents. If the connection cannot be established based on review of the provided documentation, the submission should be rejected.

A commonly-expressed request by rights holders is the option to submit rights data to the Clearinghouse either directly, or by use of an agent (i.e., a party engaged to act on the rights holder's behalf for this purpose). Feedback also suggested that some users may have a high volume of submissions, calling for the availability of a bulk submission tool.

It was also considered whether agents submitting data to the Clearinghouse would need to be accredited or obtain credentials for doing so. This could be desirable in some respects (e.g., may cut down on risk of false submissions).

However, this will not be required given that the submission of rights for authentication is intended to be a clear and straightforward process, and there is no requirement limiting who a rights holder may authorize to act on its behalf.

The optimal level of scrutiny with regard to a submitting party was considered in reference to the risk of invalid or unauthorized submissions of accurate rights data. Penalties should be in place to help deter fraudulent submissions – for example, banning a party from future Clearinghouse submissions, or reports to law enforcement. (In any case, a determination that a submission was fraudulent should result in removal of the record from the Clearinghouse.)

2.1.3 Mark Information

The trademark string (i.e., the word mark exactly as it is registered with the appropriate jurisdictional trademark authority or is protected by statute, treaty, or validated by court proceeding) must be entered in its native form (using the Unicode character set). This is necessary for accurate representation and transmission of the trademark string.

Although a broader set of rules for Identical Match is applied to identify matching domain names for purposes of Sunrise and Trademark Claims services (as discussed in section 5), only the mark as listed by the issuing jurisdiction (or other supporting sources as relevant) should be entered for purposes of authenticating the submission.

2.1.4 Contact Information

The ability for the Clearinghouse to communicate with the submitter through electronic means is of primary concern. At a minimum, an email verification step is recommended whereby the Clearinghouse will transmit information to the electronic contact provided, such that the contact must respond within a fixed period of time to confirm the accuracy of the address. Confirmation of the contact information should occur periodically and must occur at least once annually. This annual confirmation may occur as part of the renewal of the Clearinghouse record (see section 2.3.2).

Additional contact verification steps could be added as determined appropriate, depending on whether certain types of problems emerge with contact information. It is recommended that the Clearinghouse provider have discretion to implement additional accuracy measures, taking into account the costs involved and the benefit derived from the extra steps instituted.

2.1.5 Required Declaration

This would consist of a sworn statement that the information submitted is true and current and has not been supplied for an improper purpose. Submitters must attest to the accuracy and completeness of the data submitted, and acknowledge responsibility for timely corrections and updates to data.

2.1.5 Registration Numbers (where applicable)

In the case of a registered trademark, relevant registration numbers submitted to the Clearinghouse must match the numbers identified on records in the issuing jurisdiction. Such data can be confirmed by reference to the issuing office. Some jurisdictions have such data available online. For those that do not, contact should be made by the Clearinghouse to confirm the accuracy of the data.

However, a principle of equitable treatment should be adopted. The steps required of similarly situated rights holders should be essentially the same regardless of whether the relevant jurisdiction makes trademark data available in an online database.

2.1.6 Statute or Treaty Information (where applicable)

The Clearinghouse will also perform a review of the treaty or statute for those marks that identify a treaty or statute as the basis of submission. In such cases, submitters will need to properly identify the relevant instruments and provide a copy of the relevant language, as well as the date of the treaty or effective date of the statute. In some cases, the Clearinghouse will be able to refer to official, public data sources (e.g., http://treaties.un.org/Home.aspx) for confirmation of the information submitted.

If the statute or treaty is not properly identified, it is not recommended that the Clearinghouse be required to find the right authority. A submission lacking proper identification should be simply rejected without prejudice to resubmission with the required information. (Note that in every case, the rejection notice must describe the deficiency of the submission.)

Correspondingly, it is not recommended that the Clearinghouse be asked to interpret a statute or treaty that is submitted; it must appear on the face of the authority clamed as a basis, that it confers the rights.

2.1.7 Documentation from Court Proceedings (where applicable)

For submissions relying on court proceedings as the basis for the submission, it is recommended that the Clearinghouse verify that the court existed as of the date of the order or judgment and that the order has the indicia of authenticity (i.e., it is signed by a judicial officer, it names the parties that were the subject of the proceedings, it confers a grant of rights).[3] The authentication process should not be an inquiry into the underlying legal basis for a court proceeding.

If the submitter is relying upon a court order to establish rights, it should appear on the face of the materials submitted that a court conferred such rights, i.e., the documentation should indicate that the relevant party has rights to a specific mark for a class of goods or services. Further, there should be evidence that the court has entered the order or judgment. A simple court document or pleading without evidence that a Court approved, adopted or entered the order or judgment should not be sufficient.

Legal interpretation cannot be the basis for the submission. As above, it is not recommended that the Clearinghouse be asked to interpret court documents submitted; it must appear on the face of the authority clamed as a basis, that it confers the rights.

2.1.8 Other Marks Constituting Intellectual Property

It is envisioned that a registry might choose to offer protection to other types of indicia that constitute intellectual property and that are capable of being authenticated. While the specific cases may vary, it is recommended that a

[3] It should not be required for the submitter to obtain a newly-signed copy of the order, only that the order must originally have been signed.

similar approach be adopted: it should be readily apparent that the rights claimed are conferred on the basis of the information submitted.

2.1.9 Options for Use of Data

At the time that rights data is submitted to the Clearinghouse for authentication, submitters will have the ability to select between: a) an option providing for use of the submitted data only for the services that are required in all new gTLDs (Sunrise and Trademark Claims), or b) an option providing for use of the submitted data for ancillary services that may be offered as well as the required services.

2.2 Validation for Proof of Use

A trademark holder must demonstrate use of a trademark to establish eligibility to participate in Sunrise registration processes. Validation for proof of use is not required for recording data in the Clearinghouse, nor for participation in the Trademark Claims service. Validation of a Clearinghouse record for proof of use is required for sunrise domain registration eligibility, as shown below:

	Rights are unauthenticated	**Rights are authenticated**	**Rights are authenticated and validated for proof of use**
Recorded in Clearinghouse	Not eligible	Eligible	Eligible
Participation in Trademark Claims service	Not eligible	Eligible	Eligible
Sunrise domain name registration	Not eligible	Not eligible	Eligible

For validation of marks by the Clearinghouse, the rights holder shall be required to provide evidence of use of the mark in connection with the bona fide offering for sale of goods or services prior to application for inclusion in the Clearinghouse. Acceptable evidence of use will be: a) a signed declaration, and b) a single sample of current use, as described in this section.

It is recognized that use requirements for trademarks vary across jurisdictions. However, a single standard must be applied by the Clearinghouse regardless of the jurisdiction where the trademark was issued. This provides that rights holders from all regions are asked to follow the same process.[4]

2.2.1 Role of Clearinghouse in Validation

A clear set of standards for validating proof of use is required. A process that minimizes subjective reviews by the Clearinghouse will serve these goals and will also help to minimize the costs for Clearinghouse users.

As described above, a key requirement is for the Clearinghouse to serve rights holders from all regions of the world. The processes and requirements for validating rights data must be accessible to and communicated to prospective users in all regions. A single standard is desired to create an efficient and predictable process, to avoid confusion, and to provide consistent treatment to rights holders across all global regions.

2.2.2 Declaration

While all parties submitting records into the Clearinghouse will make a declaration concerning the accuracy and completeness of the data submitted (see section 2.1.5), a standard form of declaration specifically concerning the proof of use documentation will be required where a record is validated for proof of use. The recommended declaration will contain the following:

The [Trademark Holder/Representative/Licensee/Agent] hereby certifies that the information submitted to the Clearinghouse, is, to the best of [Trademark Holder/Representative/Licensee/Agent's] knowledge complete and accurate, that the trademarks set forth in this submission are currently in use in the manner set forth in the accompanying specimen; that this information is not being presented for any improper purpose; and that if, at any time, the information contained in this submission is no longer accurate, the [Trademark Holder/Representative/Licensee/Agent] will notify the

[4] See discussion of this requirement at http://archive.icann.org/en/topics/new-gtlds/trademark-protections-evidence-use-07jun11-en.pdf.

Clearinghouse within a reasonable time of that information which is no longer accurate, and to the extent necessary, provide that additional information necessary for the submission to be accurate. Furthermore, if any Clearinghouse-validated mark subsequently becomes abandoned by the holder, the holder will notify the Clearinghouse within a reasonable time that the mark has been abandoned.

2.2.3 Sample of Use

The baseline standard used for proof of use samples is intended to be flexible to accommodate practices from multiple jurisdictions. It is recommended that the sample be an item that evidences an effort on behalf of the holder to communicate to a consumer so that the consumer can distinguish, without the possibility of confusion, the products or services of one from those of another.

Examples of such evidence would include: labels, tags, containers, marketing materials, advertising, brochures, or screen shots.[5]

Mere inclusion of a mark in a domain name will not constitute use, nor will email messages or blog postings.

Given the need for flexibility, other forms of evidence that could be considered include:

- Applications for business licenses that include the mark as part of the business name
- Letterhead
- Licenses to use the mark in question
- Catalogs
- Manuals
- Displays
- Pamphlets
- Infomercial/video presentation excerpts
- Electronic display
- Press release
- Business cards
- Social media marketing materials

[5] It is not expected that physical copies would be required: links, copies, or photographic submissions would be acceptable.

The sample submitted must contain the trademark string being validated. The Clearinghouse should not assume the role of making determinations on the scope of rights associated with a recorded trademark or the labels it can generate.

2.3 Updates and Renewals of Clearinghouse Records

The data stored in the Clearinghouse should be as accurate, up-to-date and complete as reasonably possible. Therefore, it is necessary to identify the relevant processes and requirements to ensure that Clearinghouse data can be updated and accuracy maintained.

2.3.1 Updating a Record

Practices should support the Clearinghouse objective of maintaining accurate data, balancing this with avoiding an overly onerous set of data maintenance requirements which reduce the market viability of Clearinghouse services.

Update processes should be flexible to accommodate various types of changes. Capability for use of appropriate account credentials to change information in a user interface should be a minimum requirement, for those fields where updates can be automated. A higher level of security, with some fields locked pending verification of a change request by the Clearinghouse, may be desired in some cases (e.g., review of supporting documentation or a notice to the rights holder confirming the updates).

At the time of submission, the rights holder will have attested that it will keep the information supplied to the Clearinghouse current so that if, during the time the record is included in the Clearinghouse, a trademark registration gets cancelled or is transferred to another entity, or, in the case of a court- or Clearinghouse-validated mark the holder abandons use of the mark, the rights holder has an affirmative obligation to notify the Clearinghouse. Penalties for failing to keep the information current can include removal of a record (with the ability to resubmit). However, there should be a reasonable amount of time for a rights holder to submit a change before penalties are incurred.

Additional processes (e.g., automated tools, audits for accuracy) could be instituted by the Clearinghouse to enhance data accuracy as considered appropriate.

2.3.2 Renewing a record

An authenticated Clearinghouse record should be renewed once per year, including confirmation of the associated contact information. Feedback suggested that renewal could incorporate a process with an annual confirmation that the record is still accurate. The renewal process would consist of the appropriate renewal fee and the required confirmation from the submitter.[6]

The renewal process should not require resubmission or re-authentication of information that was previously provided. (The opportunity to challenge the admission of a Clearinghouse record should continue to be available, as noted in section 4.1.)

With regard to validated records (i.e., Clearinghouse records that have been validated for proof of use), it is recommended that the annual renewal for the record not require submission of a new sample. However, submission of a current sample should be required at a longer interval (e.g., every five years) to ensure that the validation data is also relatively current.

If a user has many records in the Clearinghouse, a form of synchronization service might be developed to support tracking of renewals.

2.4 Removal of Clearinghouse Records

A record may be removed from the Clearinghouse database under circumstances such as:

a. Notice of that a trademark has been abandoned.

b. A request from the rights holder to delete the record.

c. The result of a dispute resolution process concerning the record.

d. Expiration of the Clearinghouse record without renewal.

[6] There were some suggestions that the expiration of a Clearinghouse record should be matched to the expiration of the underlying trademark record in the relevant jurisdiction; however, this was considered less desirable than an annual approach in that it added complexity to the administration required by the Clearinghouse as well as the user experience.

The Clearinghouse should provide a clear timeline including at least one notice of pending expiration, using the contact information associated with the Clearinghouse record, before a record is removed for expiration. The Clearinghouse provider should publish and supply notice of any grace period procedures that are instituted.

Removal of a record from the Clearinghouse would mean removal from an active status in the database. Historical records must still be retained for audit and logging purposes for a period to be determined.

Expiration and deletion of a record will not prejudice applications for reinstatement. A set of procedures should also be available for reinstatement of an expired Clearinghouse record where certain conditions are met.

2.5 Audit and Logging Requirements

Complying with best practices and statutes for audit and compliance will require Clearinghouse information to be retained or other reporting and audit mechanisms to be implemented. Clearinghouse processes should incorporate the community requirements for retention, publication, and disclosure of Clearinghouse information where needed, including audit and logging trails.

Part 3 – Sunrise and Trademark Claims Processes

3.1 Sunrise

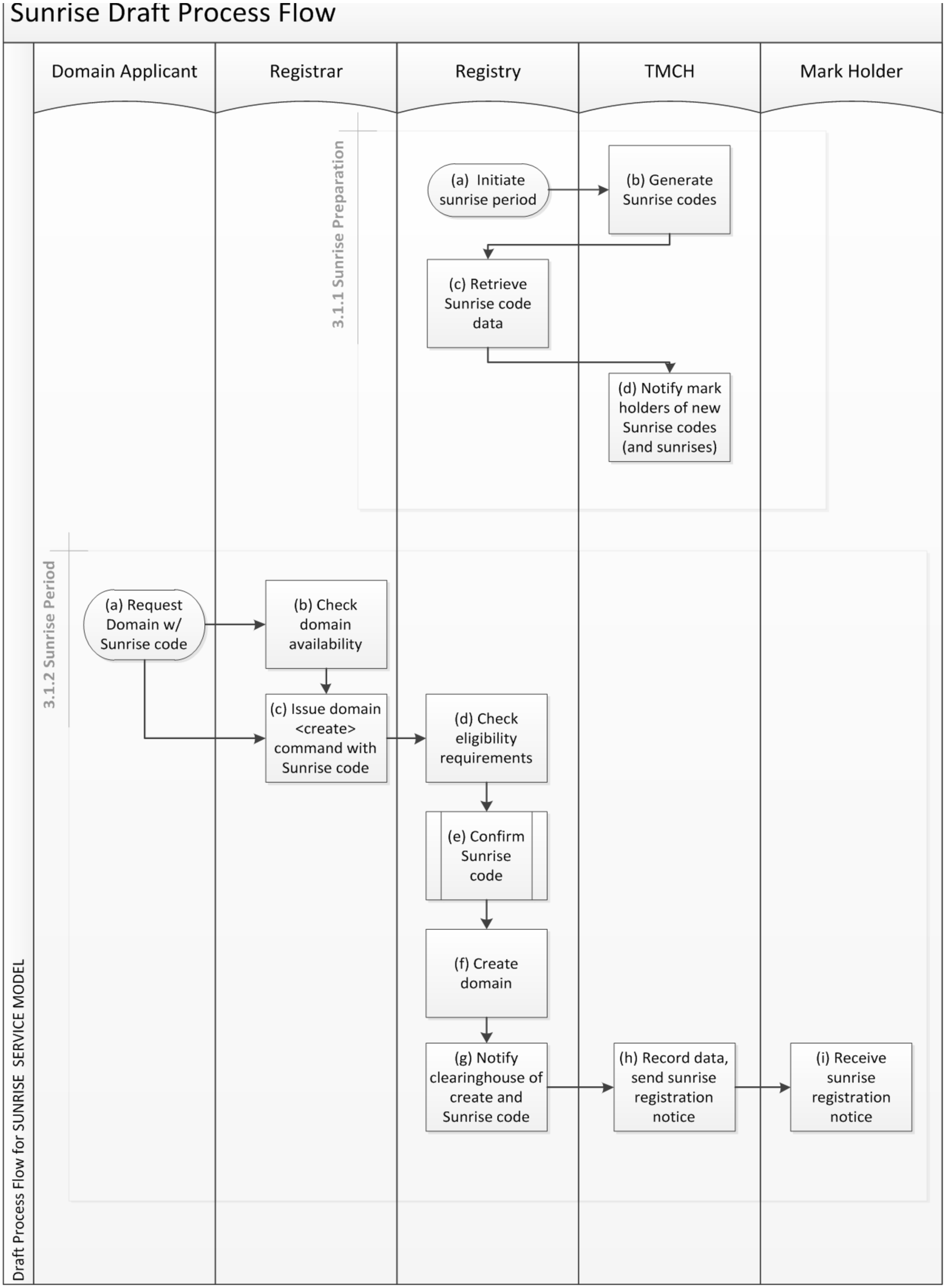
The Sunrise period provides an opportunity to eligible rights holders to register domain names in a particular TLD, before names become available for general registration. A Sunrise period of at least 30 days is required in all new gTLDs.

Registries and others have expressed a desire for flexibility to be able to configure the Sunrise period for the circumstances of the TLD launch process. The recommended model described in this section is able to accommodate a variety of approaches, including first come/first served, auctions, or other allocation methods.

The model incorporates the use of a token or "Sunrise code" issued by the Clearinghouse to indicate eligibility for Sunrise – which could then be used by the rights holder with any registrar of its choosing. Feedback indicated that the Clearinghouse's technology should not be too complicated to use. However, it was generally accepted that the use of public/private keys would not be too burdensome, and could be useful for validating requests. The Sunrise code is viewed as a way to save steps in verifying information.

A Sunrise code should be unique per mark rather than per mark holder. A need to maintain a large volume of unique codes creates some administrative responsibility; however, feedback indicated that it was important to associate a specific trademark record to the Sunrise period registration, and this would be difficult to do if there is no unique code associated with each Clearinghouse record. From the perspective of the Clearinghouse, either approach could be implemented; however, the code also needs to identify matching domain names associated with the record.

See the Sunrise process diagram and description of steps below.


Sunrise Draft Process Flow
Domain Applicant
Registrar
Registry
TMCH
Mark Holder
3.1.1 Sunrise Preparation
(a) Initiate sunrise period
(b) Generate Sunrise codes
(c) Retrieve Sunrise code data
(d) Notify mark holders of new Sunrise codes (and sunrises)
3.1.2 Sunrise Period
(a) Request Domain w/ Sunrise code
(b) Check domain availability
(c) Issue domain <create> command with Sunrise code
(d) Check eligibility requirements
(e) Confirm Sunrise code
(f) Create domain
(g) Notify clearinghouse of create and Sunrise code
(h) Record data, send sunrise registration notice
(i) Receive sunrise registration notice
Draft Process Flow for SUNRISE SERVICE MODEL

3.1.1 Sunrise Preparation

In this model, steps occur as follows:

a) Registry schedules Sunrise period dates.

b) Clearinghouse generates Sunrise codes for all validated Clearinghouse records. The length specification for a Sunrise code is not yet defined, but will balance the needs for protection of the data and usability by rights holders. The Sunrise code will have certain cryptographic characteristics, so that it can be broken into pieces: part can be shared with the rights holder, and another part can be shared with the registry. Only when all the pieces are properly combined will the code be capable of demonstrating the validity and authenticity of the code; no individual piece is sufficient to derive the other.

c) Registry retrieves its Sunrise code data as provided by the Clearinghouse for the relevant TLD.

d) Clearinghouse notifies applicable rights holders that new Sunrise codes are available (e.g., "New codes are now available for the upcoming Sunrise registration period in TLD.") The notice is factual in nature and does not promote the TLD or provide registry-specific information.

3.1.2 Sunrise Period

In this model, steps occur as follows:

a) Applicant requests domain name, provides Sunrise code to registrar.

b) Registrar checks domain availability (optional step depending on registrar model).

c) Registrar issues domain <create> to Registry, with EPP extension to include Sunrise code.

d) Registry checks eligibility requirements.

e) Registry confirms that the Sunrise code is authentic and issued for the domain name requested.

f) Registry creates domain and responds to Registrar as appropriate (either a confirmation of creation or a rejection of the <create> command with appropriate error notifications). (Registrar would then provide notification to applicant).

g) Registry notifies Clearinghouse of domain registration.

h) Clearinghouse sends notice of Sunrise registration to relevant rights holders.

i) Rights holders receive notice. Sunrise codes provided to Registry are not used after the completion of the Sunrise period.

3.2 Trademark Claims

The Trademark Claims service provides a real-time notice to a party attempting to register a domain name that matches a Clearinghouse record, as well as notifying relevant rights holders when a domain name is registered that matches a Clearinghouse record. The Trademark Claims service must be offered until the end of the first 60 days of general registration in all new gTLDs.

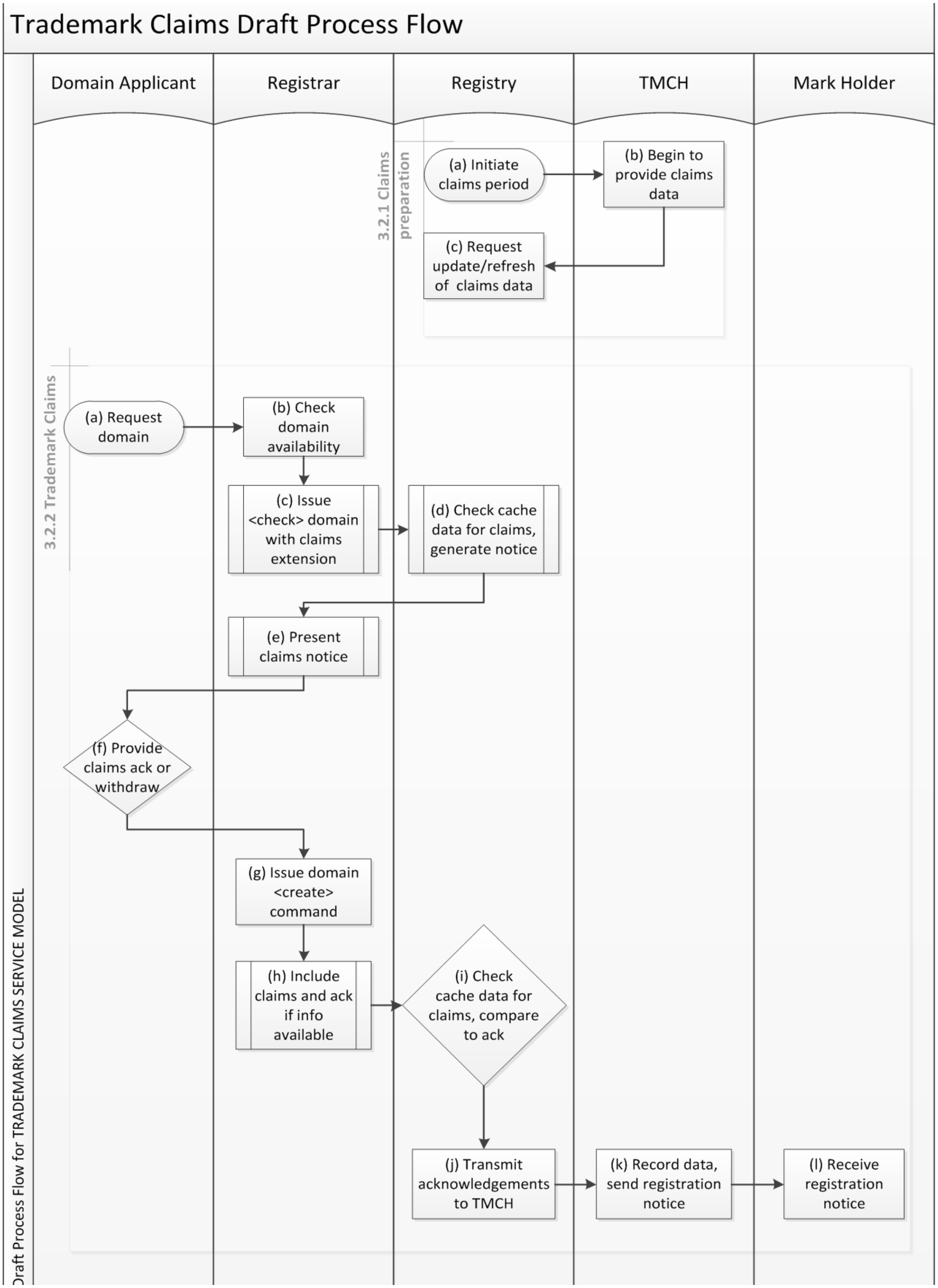
Establishment of communication channels for the Trademark Claims service was extensively discussed pertaining to the involvement of the Registry and the Registrar in the registration process, and how communications with the Clearinghouse should occur.

It was considered desirable to have only one party interacting with the Clearinghouse. For regular communications pertaining to registrar activity, it is envisioned that most communications would go from the Registrar to the Registry, to the Clearinghouse.7

For any communications involving the domain name registrant, however, it is recommended that the registrar own that communication. The Registry as primary communicator with the Clearinghouse, and the Registrar as primary communicator with prospective domain name registrants, maintains a principle that each party should interact with the party to whom it is closest in the chain. Introducing communications from multiple or unexpected parties in to the process was considered contrary to the goals of maintaining an efficient registration process.

See the Trademark Claims process diagram and description of steps below.

[7] This is without respect to a registrar who might also function as a service provider that interacts with the Clearinghouse as an agent, separately from its role as a registrar.


Trademark Claims Draft Process Flow
Draft Process Flow for TRADEMARK CLAIMS SERVICE MODEL
Domain Applicant
Registrar
Registry
TMCH
Mark Holder
3.2.1 Claims preparation
(a) Initiate claims period
(b) Begin to provide claims data
(c) Request update/refresh of claims data
3.2.2 Trademark Claims
(a) Request domain
(b) Check domain availability
(c) Issue <check> domain with claims extension
(d) Check cache data for claims, generate notice
(e) Present claims notice
(f) Provide claims ack or withdraw
(g) Issue domain <create> command
(h) Include claims and ack if info available
(i) Check cache data for claims, compare to ack
(j) Transmit acknowledgements to TMCH
(k) Record data, send registration notice
(l) Receive registration notice

3.2.1 Claims Preparation

In this model, steps occur as follows:

a. Registry schedules Trademark Claims period.

b. Clearinghouse provides claims data to registry.

c. Registry requests update/refresh of claims data from Clearinghouse.

3.2.2 Trademark Claims

In this model, steps occur as follows:

a. Applicant requests domain name from participating Registrar.

b. Checking of domain name for claims, as described below.

c. A Registrar will submit a <check> command for the domain name (using EPP extension for trademark claims).

d. The Registry must determine whether claims exist.

e. In cases where claims exist, the registry decrypts and constructs the trademark claims notices for inclusion in the EPP response to the registrar's <check>.

f. If presented with trademark claims notice, a domain name applicant must acknowledge the claims through some active action (checkbox or other affirmative step), or cancel the request for the domain name. That acknowledgement must be captured by the Registrar, along with identifying information about the acknowledgement.[8]

g. Registrar transmits a domain <create> command to Registry.

h. If trademark claims exist (i.e., claims data was sent to Registrar), then claims data, along with the acknowledgement from the applicant, must be included in the EPP (domain <create>) command from the Registrar, using trademark claims extensions. Failure to include this

[8] The Trademark Claims notice contains the following: "If you continue with this registration, you represent that, you have received and you understand this notice and to the best of your knowledge, your registration and use of the requested domain name will not infringe on the trademark rights listed below. This is acknowledged by the domain name applicant in this step. If no acknowledgement occurs, the registration does not proceed.

information during the trademark claims period must cause the Registry to reject the create command with an appropriate error code.

i. The Registry must check all domain <create> commands for claims during the Trademark Claims period. The requested domain must be checked for the existence of trademark claims. If there are claims, and either no claims acknowledgement has been transmitted to the Clearinghouse or the claims acknowledgement does not match the claims data available to Registry when the domain <create> is processed, then the <create> command must be rejected. It is the responsibility of the Registry to ensure that no domains are created with mismatched or missing trademark claims acknowledgements.

j. The Registry must transmit acknowledgement data to the Clearinghouse.

k. The Clearinghouse records acknowledgements and domain <create> events. This information provides both the audit trail of the Trademark Claims period and triggers the Clearinghouse transmissions domain registration notices.

l. The Clearinghouse transmits domain registration notices to relevant rights holders.

3.3 Audit and Logging Requirements

Complying with best practices and statutes for audit and compliance may require information regarding trademark claims and Sunrise processes to be retained or other reporting and audit mechanisms to be implemented by the Clearinghouse, registries, and registrars. These processes should incorporate the community requirements for retention, publication, and disclosure of Clearinghouse information where needed, including audit and logging trails.

Data concerning, for example, the acknowledgement or transmission of a Trademark Claims notice may be relevant information in various types of disputes; this data must be available when needed to inform such an inquiry.

3.4 Communications Protocols

The feedback received suggested that EPP should be used for all communications between the Registry and Registrar, since this is already known and used by gTLD registries and registrars. EPP for communications between registries and registrars has been retained in this model; however, extensions will be needed to accommodate the Sunrise and Trademark Claims data.

Mandatory protocols include:

a. EPP domain <check> during the Sunrise 3.1.2(b) transaction.

b. EPP domain <create> during the Sunrise 3.1.2(c) transaction (requires an EPP extension to include sunrise codes)

c. EPP domain <check> during the Claims 3.2.2(b) transaction (requires an EPP extension that requests trademark claims data, if available)

d. EPP domain <create> during the Claims 3.2.2(g) transaction (requires an EPP extension for trademark claims)

Protocols for Registry communications with the Clearinghouse, recommended in this model, leverage synergy between the transmission and receipt of information through the use of Rsync over an SSH transport to transmit properly formatted data files. The rationale and detailed model are described in this section.

3.4.1 Protocols to Retrieve Data into a Local Cache

The recommendation for retrieval of Clearinghouse data is as follows:

Registry retrieves information from the Clearinghouse	Using Rsync on an SSH transport (to ensure point-to-point encryption and endpoint authentication), the registry will retrieve data in the following structure. There will be read-only repositories for Trademark Claims data and for Sunrise data, so that the registry can retrieve data, but cannot send data to this repository. Within the Sunrise repository, Sunrise codes will be stored with one file named the same as the Sunrise code lookup value. Each file must contain the initial effective date of the

	Sunrise code. Within the Trademark Claims repository, claims notice data will be stored in files named with the lookup code, one file per claims notice structure. File and directory names must fall within RFC4648 BASE32 encoding, as the underlying operating systems and file systems may not properly reflect case sensitivity. (It would be otherwise desirable to use URL-safe BASE64, but that requires an assurance from registry providers we presently do not have). A multi-level directory structure will be used in the read-only repositories. The top level will contain a directory for the first byte of each BASE32 encoded string in the repository. The second level will also contain a directory for the second byte of each BASE32 encoded string in the repository, etc. This approach must be used for the first three levels, so that an encoded string ABCDEFG would be stored in an rsync directory structure of A/B/C/ABCDEFG. Unnecessary directories (directories without at least one file entry) must not be created and should be removed.

Transaction 3.1.1(c), more generally described as Sunrise data retrieval (from Clearinghouse to registry), and transaction 3.2.1(c), more generally described as Claims data retrieval (from Clearinghouse to registry) could occur using one of the following protocols:

- HTTPS encrypted payload to local cache
- Rsync encrypted payload to local cache
- DNS zones with encrypted labels and payload

While the data retrieved during the Sunrise and Trademark Claims transactions serves different rights protection mechanisms, these retrieval functions are, from a protocol standpoint, almost identical: the technical problem of synchronizing two data repositories to both contain the same information in a bandwidth-, time-, and computationally efficient manner is the same. The organization of data involved (lists with a single key for lookups, that reference arbitrarily sized, formatted results) are also extremely similar. Thus, as a matter of implementation efficiency, these transactions should occur using the same retrieval protocol.

The option considered for use of a DNS zone model was based on the Clearinghouse operating services used in real-time to ensure that rights protection functions occur; the recommended design is instead based on periodic updates to information from a central source so that registries are shielded and resilient against Clearinghouse technical failures. The DNS option provided for a partial integration of lookup and distribution services. Unfortunately, there are substantial technical difficulties due to a limitation in the maximum size of DNS data objects (64 KB) which could be exceeded for trademark claims data. This problem, while not impossible to resolve, requires extending the DNS protocol with a new query type and structuring that data to identify the "chains" of DNS queries needed to transfer larger data sets. Ultimately, while innovative, mandating specific and substantive changes to the internals of how a registry would be implemented (rather than establishing workflow requirements) seems unwise: local caching does not require mandating specific mechanisms and protocols to perform internal lookups of data; this is appropriate for the registry to handle and an appropriate delegation of that responsibility.

Using HTTPS or Rsync allows the responsibility of resiliency to be fully undertaken by the registry. This separates data distribution from lookups. From an engineering standpoint, the lookup functionality might be better-served in some other database system than DNS. Rather than extend the DNS protocols, providing the Clearinghouse data in a fixed format and letting the registry determine the best way to implement Clearinghouse lookups and functionality seems expedient and efficient. Between the options of HTTPS and Rsync, Rsync is suggested simply because it's designed for the specific purpose of efficiently synchronizing data between remote data sources. Using Rsync also means less protocol specification and ultimately gives greater flexibility to support a wider range of registry implementations.

3.4.2 Protocols to Send Data to the Clearinghouse

The recommendation for sending domain data to the Clearinghouse is as follows:

Registry sends information to the Clearinghouse	Using Rsync on an SSH transport, the registry will push data to the Clearinghouse. There will be a read/write repository per registry, so a given registry cannot interact with files from other registries. On the registry side, the registry must ensure that each filename is unique: filenames must not be reused. The registry should only attempt to synchronize files until they are successfully sent. On the Clearinghouse side, the Clearinghouse must not permit overwriting or deletion of files.

Transactions 3.1.2(g) and 3.2.2(j), which communicate from the Registry to the Clearinghouse specific details relating to domain creations, are also almost completely identical. The functionality is similar to functions provided in EPP; however, registries do not generally integrate the EPP client-side into their registry operations (they operate as EPP servers to registrars). With EPP appearing to require substantial new implementation for the registry in this respect, and the functional need to inform people being driven by human (rather than fully automated) decision and reaction times, moving to a different, simpler protocol is both reasonable and appropriate. These protocols which transmit transactional data from a registry to the Clearinghouse could thus be handled using one of two protocols:

- HTTPS PUT of an XML payload (including ReST, JSON, AJAX, OGDL, etc)
- Rsync of an XML payload

Using Rsync would structure the Clearinghouse as a batch-processing environment (rather than a real-time environment). Update speeds would be a function of the frequency and runtime of Rsync runs, which in turn are driven by policy and procedure statements rather than technical characteristics. The use of Rsync also eliminates almost all network protocol dependency for the Clearinghouse functionality, and relies on a deployed, stable, and reliable synchronization protocol. An Rsync approach forces easy queuing of messages for processing, but will require management of processing latency.

Under the proposed workflows and responsibilities, the Clearinghouse does not sit inline during the registration process: rights protection services are performed by the registry, informed by data provided on a regular and periodic basis from Clearinghouse. The expectation is that as the data set becomes larger (the transfer protocol design is scaled to handle several million protected labels), the refresh of data from the Clearinghouse will always occur at least once per day and that Clearinghouse will receive data from the registries so that the processing latency for trademark claims remains below 6 hours.

HTTPS would be friendly to real-time Clearinghouse processing (claims and Sunrise notices could occur more promptly). However, this also creates the need for a large and expensive production-grade processing operation or forces the registry to be able to queue failed transactions for later.

3.4.3 EPP Protocol Extensions

There are several extensions required to two EPP commands that operate between the registrar and registry.

- EPP <create> Command

The <create> command must be extended in two ways. Two new components of payload object data need to be able to be included and processed by the EPP processing component.

a. Sunrise code as provided by domain name applicant
b. Trademark Claims acknowledgement data

Responses to the <create> may need to include new or extended error codes, or may use some already existent response codes to indicate that the name could not be registered because of lack of Trademark Claims acknowledgement.

- EPP <check> Command

The <check> command must be extended so as to specify that the EPP client is capable of receiving trademark claims extensions responses, and so that claims data can be returned. The request should permit two modes of query:

a. A “lightweight” check, which is used to determine only whether one or more claims exist.
b. A “heavyweight” check, which asks for the full trademark claims notice data.

The response to this <check> command would then contain one of the following:

a. Structured claims data

b. A reply that indicates that no claims exist

c. A reply that indicates that one or more claims exist.

3.4.4 Data Structures (EPP enhancements and external data structures)

An <ack> (acknowledgement) would be constructed as:

```
<ack> // ack object is for claims acknowledgements
  <registrar>
  <registrant> // registrant object - contact (rfc5733)
  <timestamp>
  <where>  // ip, phone, or address
  <fqdn>
  <sunrisecode> or <notice>
</ack>
```

A <notice> (which can be used in EPP extensions or in the ack above) would be constructed as:

```
<notice id="label">
  <claim>  // zero or more claims may be included in a notice
    <mark>
    <owner>
    <contact>
    <class>
    <jurisdiction>
    <goods>
  </claim>
  </notice>
```

3.5 Data Locations and Data Access

To minimize abuse, distribution of Clearinghouse data is limited to situations where necessary to implement required functionality.

Specifically, some rights holders indicated concern that the aggregation of rights data through the Clearinghouse may expose corporate strategies or be used to gather competitive intelligence, particularly if the database is freely searchable and accessible. For example, it might be possible to identify jurisdictions in which a rights holder has not registered its trademarks or in which it has not chosen to register domain names. In this regard, this information could drive uses such as phishing or other types of social engineering activities.

Accordingly, consideration is given in the model to minimizing the potential for data mining. It was recommended that the Clearinghouse model should apply varying levels of technological and contractual restrictions depending upon the type of data accessed and the sensitivity of the data, and this is taken into account.

Some Registries and Registrars expressed as a requirement that the uptime and performance of the registration process not be negatively impacted by insufficient or unavailable data from the Clearinghouse. Accordingly, the model provides that the subset of data required for Trademark Claims and Sunrise can be provided to the registry (here, in a hashed form) and regularly updated, so that parties providing domain name registration services can rely on the data without having to query the Clearinghouse.

3.5.1 Local Caching at Registry

The service-level commitments of a registry are substantial, and this informs the goal to avoid introducing new third-party technical dependencies into the operations of the registry. This could, with sufficient cost and effort by the Clearinghouse (and thus additional cost to rights holders and registries), be addressed by making operation of the Clearinghouse large and highly distributed. However, a method that could be just as technically effective and would be custom fit to each registry's operation would be to provide a copy of the necessary information to perform the required functions to each registry. Given that rights holders have expressed privacy and data access concerns about broadly distributing that information in clear text, this document describes a technical method by which the Clearinghouse can provide the necessary information in such a way as to strongly resist misuse and abuse.

3.5.2 Cryptographic approach

As noted above, there are two difficult technical demands placed on the Clearinghouse. The first is to ensure that the Clearinghouse does not introduce third-party technical disruptions to the domain name registration process. That is, registries and registrars don't want to be dependent on the technical effectiveness and uptime of the Clearinghouse.

The second is the demand that information not be broadly distributed (as an attempt to prevent exposure of data that may be subject to misuse). Data mining can be made computationally expensive and unprofitable through the use of cryptography.

Through the cryptographic approach using the prescribed methodology described below, the following results are achieved:

- Only the Clearinghouse and the rights holder have access to Clearinghouse records.

- There is no plaintext list of labels or Sunrise codes provided by the Clearinghouse. Labels and Sunrise codes are, instead, transformed using a specified mechanism.

- Access to Clearinghouse records is limited to all and only the information required for trademark claims, and only for those labels which are known to the registry (having been communicated to the registry from a registrant by way of a registrar).

- Sunrise codes are single-use, so as to control the risks posed by re-use.

- hmac(key,payload) would generate an HMAC-SHA1/SHA256/SHA512 of payload.

- aes(key,payload) would generate the AES128/AES256 encrypted result of payload, encrypting with key.

- secret() refers to a shared secret that exists between the Clearinghouse and a specific registry.

- A trademark string refers to the word mark exactly as it is registered with the appropriate jurisdictional trademark authority or is protected by statute, judicial decision or treaty.
- "Label" refers to a potentially valid DNS label generated from a Clearinghouse-listed trademark string using the "identical match" rules described in the gTLD Applicant Guidebook. Applicants would wish to register label.tld.

Exact encryption key and Sunrise code sizes and the specific complexity of the established strong encryption algorithms are not yet set: community comment is both invited and welcomed to help clarify the balance between computational cost/speed of processing for registries and the value of Clearinghouse data to attackers. However, the reference examples in this document were generated using 128 bit secret keys using HMAC-SHA1 and AES256 as the algorithms. Sunrise codes were generated by creating 128 bit pseudorandom numbers.

Transaction	**Prescribed Methodology**	**Security Result**
Verification of a Sunrise code	Use hmac(secret(),sunrisecode.label.tld). The default encoding of this lookup string must be RFC 4648 compliant BASE32. Registry will access locally cached information originally sourced from the Clearinghouse; cache management is handled in a different transaction.	The only way to obtain the mark holder's Sunrise code out of the hmac code is to know the mark holder's Sunrise code and the label and TLD it applies to. HMAC (hashed message authentication code) functions are a method to ensure data integrity and authenticity of a message. Used in this way, we can prevent exposure of sensitive data required for matching purposes, except in those cases

Transaction	Prescribed Methodology	Security Result
		where we already know exactly what we're matching. This means that sunrise codes must, at a minimum, be specific to the label, mark holder and gTLD involved. They should also be unique across all matching labels and gTLDs. During the Sunrise period, the only Clearinghouse information available to a registry is a list of hmac(secret,sunrisecode.label.tld). No trademark strings or sunrise codes are available.
Determination that a domain name is subject to trademark claims	Use hmac(secret(),label.tld)as the lookup string. The default encoding of this lookup string must be RFC 4648 compliant BASE32. Registry will access locally cached information originally sourced from the Clearinghouse; cache management is handled	The only way to see a label is to have both the shared secret and the label.

Transaction	Prescribed Methodology	Security Result
	in a different transaction.	
Retrieval of trademark claims data	The return value should be aes(hmac(secret(),label),claims data). The lookup should be based on the lookup string for determining that a domain name is subject to trademark claims.	The only way to get access to the claims data is to have the label it refers to already. This is the legitimate use case. No additional information is available without knowing what you're looking for.

Maintaining control and limiting disclosure of Clearinghouse data is a very high priority. The cryptographic model as a mandatory access and procedural control significantly limits the exposure of Clearinghouse data to only those cases where the usage appears legitimate. In this model, the only way to get sensitive data is to have most of the sensitive data available already:

- Sunrise codes come in two pieces. The registrant has a code, which he presents to a registrar in conjunction with a fully qualified domain name he wishes to register: that code is confirmed to be authentic by the registry, and that act of confirmation is in turn verifiable by Clearinghouse. The only known way to bypass any of these checks is to know or guess the custom codes held by the registrant and registry.
- The list of Clearinghouse available labels is protected such that the only way to see whether a particular label is protected is to know that label. There is no known method by which to scan the list for similar labels or mine the lists without first having the specific labels you want to know about.
- Trademark claims notice data is obfuscated such that the only way to see the claims notice data is to check based on a specific mark. The list cannot be scanned, searched or mined without first defeating strong encryption.

While there is a brute force vulnerability (trying all strings), that vulnerability is inherent to the trademark claims service, not specific to this approach, and would exist even if the data were not distributed. That behavior needs to be controlled through contract, audit and compliance activities.

Examples of the described functionality are included below.

Code component	**Value**
Top level domain	Test
Label	Example
Fully qualified domain name	example.test
Registry-Clearinghouse shared secret	14949998966411241762412357844692506274

Sunrise data	**Value**
Mark holder is given the following code by the Clearinghouse	158615152027740804575624053394539103379
Registry receives the following Sunrise lookup code (base32)	OEGNQPZOUFRZ7CH3IBL5HRAUI6K3UPFV

Trademark Claims data	**Value**
Registry receives the following trademark claims lookup code (base32 version)	6SABLA74ATT5IZZK2MTEBHDYANGAD4MK
Simplified example of plaintext of trademark claims data	<notice id="example"> <claim> <mark>example</mark> <owner>Example Corporation</mark> <contact>Example Contact, city, state/province/etc, country</contact>

	<class>42</class> <jurisdiction>DE</jurisdiction> <goods>An example</goods> </claim> </notice>
Trademark claims as seen by registry	U2FsdGVkX1/EnR9IOyHTdqaCPRTWkVuvSTYlNa4OttFY FleNWJHALR4SjbXC+VVe Feh/Sgt1myjx1FNRbfnWBZV+F3XTUgMc6CbRuSl4SqJVEu hIpo8EZeH+LSKgAof2 rC/nhZum2osIAuQfSknaUI5MffFCjLNPGB16DqpPwg5OS AEkfkHNDYe3hwoo92El MX5xmzAVuF7AcbYi+R92U0FumOnDTypl3Sw39j9r2tsT6z x+ndpW22yxIM2rFmtN whLieqfiN47RfDTTIbAlGA==

3.6 Extending Mandatory Rights Protection Mechanisms

The trademark claims period is mandatory through the first 60 days of general registration. The sunrise period is mandatory for 30 days prior to general registration. However, it is expected that some registries might wish to extend the period during which they offer these rights protection services.

Overall communication protocols and workflows in this model will support many expansions, such as to time periods of claims or sunrise. Both claims and sunrise are designed around being incrementally updated after a large initial download of information. Such functions are neutral to the content of the communications, depending solely on being able to identify changes to the content.

The cryptographic controls and the assurances against fraud and abuse are largely controlled by a shared secret between the registry operator and clearinghouse. The risk profile for using a shared secret for a short period, like 4 months, is different from the risk profile for using a shared secret for a long period, like 5 years. It would limit the security of the clearinghouse data to allow a long-lived shared secret. Thus, the shared secret would need to be changed periodically, at agreed upon times between the registry and clearinghouse in accordance with some security policy.

Shared secret changes affect sunrise codes, claims periods, and claims notice data decryption, and would affect the contents of the repository. While this can be implemented through the use of shared timestamp data (assuming the registry side implementation supports timestamp synchronization in rsync), it complicates the registry operation by requiring that it be capable of supporting multiple shared secrets for the same data set. Ultimately, a shared secret rotation would result in changes across all contents of the sunrise and claims repositories. While this change could be expected to be implemented in phases so as to avoid a massive bulk update that would be time-, bandwidth and computationally expensive, it will require special procedures and handling. Any substantial variations on the established requirements will require a detailed analysis taking into account specific requirements.

Part 4 – Dispute Resolution

Disputes of various types may arise during the operation of the Trademark Clearinghouse and of processes supported by Clearinghouse data. Dispute resolution mechanisms should be in place to address these in a fair and efficient manner, based on an impartial review of the facts and circumstances.

In some cases, procedures for addressing a dispute may resemble a reconsideration or appeal process, while in other cases, a matter might be appropriate for a form of dispute resolution proceeding between parties.

Specific types of possible disputes are discussed in this section.

4.1 Disputes concerning Clearinghouse Processes

Dispute resolution mechanisms regarding determinations made by the Clearinghouse should concern adherence to Clearinghouse standards and processes, rather than issues regarding the underlying rights. The Clearinghouse should not be a venue for deciding legal claims.

Mechanisms for handling these types of disputes are expected to consist of a re-examination by the Clearinghouse, performed by a different evaluator than made the original determination concerning the record. Fees associated with this process would be at the discretion of the Clearinghouse provider, although a reimbursement of costs would be appropriate if the error is determined to be on the part of the Clearinghouse. Two types of cases for re-examination are foreseen:

4.1.1 Clearinghouse Record Accepted in Error

This is a dispute on the basis that the Clearinghouse's authentication or validation on a record was invalid, that is, that a Clearinghouse record was accepted when it did not meet the established requirements. This type of complaint would generally be initiated by a third party, not by a rights holder associated with the record.

The Clearinghouse review of such a dispute must examine whether the Clearinghouse properly applied the relevant standard.

It should be noted that this type of dispute could occur at any point after a Clearinghouse record is accepted.

In the instance where it is determined that a Sunrise registration has been permitted by a Registry due to an improper authentication or validation step by the Clearinghouse, then notification should be provided to the Registry and consideration must be given to the appropriate remedy (also taking into account Registry policy).

4.1.2 Clearinghouse Submission Denied in Error

This would be a dispute on the basis that the Clearinghouse either: a) rejected a submission for authentication, or b) rejected a submission for validation for proof of use, in error.

Again, this would require a review by the Clearinghouse of whether the relevant standard was properly applied. This type of dispute would typically be submitted by a rights holder.

4.2 Sunrise Disputes

Dispute resolution mechanisms regarding registration of domain names during the Sunrise period are also pertinent to the registry operator, which administers the registry eligibility requirements and the allocation of names during the Sunrise period. The involvement of the Clearinghouse in these cases is described below.

In each case, the Clearinghouse must cooperate with dispute resolution proceedings by providing the relevant information.

4.2.1 Registry Permitted / Denied Sunrise Registration in Error

This type of dispute would concern an action taken by the Registry. The bases for such disputes include:

a) the prospective registrant was eligible for the Sunrise registration (according to registry-specific requirements), and was not awarded it by the registry.

b) the prospective registrant was not eligible for the Sunrise registration (according to registry-specific requirements), but the Registry permitted the registration to occur.

c) an error made by the Registry in administering its Sunrise allocation mechanism.

Here, it is not the operation performed by the Clearinghouse that is at issue, but the Registry's process. It is expected that registries will have general complaint mechanisms or mechanisms available to handle such cases.

4.2.2 Notice of Sunrise Registration Not Sent

In this model, providing the notice of Sunrise registration to the relevant rights holders (i.e., notice that a domain name matching the Clearinghouse record has been registered during the Sunrise period) is the responsibility of the Clearinghouse. The Clearinghouse would require a mechanism to investigate and resolve complaints of this type.

4.3 Trademark Claims disputes

The Trademark Claims service is based on automated matching and provision of notices, rather than determinations being made by a particular party. However, disputes may occur concerning whether a notice was properly presented or acknowledged.

In this model, errors could be caused by the Clearinghouse (e.g., in application of the matching rules), by the Registry (e.g., in transmission or checking of claims data) or by the Registrar (e.g., in display of the Trademark Claims notice). All parties must have mechanisms for investigating and resolving these types of complaints.

A review of the types of disputes discussed in this section is provided in the table below.

Dispute Resolution Overview

Relevant party	Basis of dispute	Initiated by	Mechanism
Clearinghouse	Record was accepted in error	Third party	Clearinghouse re-examination process
	Record was denied in error	Rights holder	Clearinghouse re-examination process
	Notice of domain registration (Sunrise or Trademark Claims) not sent	Rights holder	Clearinghouse process

Registry	Sunrise registration was permitted / denied due to Registry error	Rights holder	Registry process
	Trademark Claims data improperly provided / not provided to registrar or Clearinghouse	Rights holder or domain name applicant	Investigation by relevant party
Registrar	Notice improperly displayed / acknowledged	Rights holder or domain name applicant	Investigation by registrar

Part 5 – Additional Considerations

5.1 Note on Ancillary Services

A Clearinghouse provider may offer ancillary services, as long as those services and any data used for those services are kept separate from the Clearinghouse database. Data in the Clearinghouse should also be licensed to competitor providers interested in providing ancillary services on equal and non-discriminatory terms and on commercially reasonable terms, where the rights holders have agreed to such use.

5.2 Matching Rules

For processing Clearinghouse records for the purpose of Sunrise and Trademark Claims processes, matching rules specified in the Special Trademark Issues Review Team recommendations[9] are used. An "identical match" is defined as follows.

Domain name consists of the complete and identical textual elements of the mark.

a. spaces can be replaced by hyphens (and vice versa) or omitted;

b. only certain special characters in a trademark are spelled out with appropriate words describing it (@ and &);

c. punctuation or special characters in a mark that are unable to be used in a domain name may be (i) omitted or (ii) replaced by spaces, hyphens or underscores and still be considered identical matches; and

d. no plurals and no "marks contained" qualify.

More work is needed on the implementation of Rule B, to determine which languages are relevant. This must balance the number of different languages in use and the difficulties of determining which languages are relevant to a given Clearinghouse record.

Where a registry may wish to institute additional matching rules, i.e., to add more characters, including IDN variant characters, this implementation should be the responsibility of the registry operator. Registries currently adopt IDN tables for a TLD

[9] http://gnso.icann.org/issues/sti/sti-wt-recommendations-11dec09-en.pdf

which may include the identification of characters considered to be variants of one another; however, there is no authoritative IDN table per script that is broadly accepted. An option for every registry to submit its own rules to the Clearinghouse was discussed, and is less desirable as it will provide an inconsistent experience for users, as well as administrative overhead which would likely be reflected in fee levels.

5.3 Costs

Costs for the Clearinghouse are to be borne by the parties using the services. It is envisioned that rights holders will pay to record data in the Clearinghouse, that Registries will pay for Trademark Claims and Sunrise services, and that registrars and others who avail themselves of Clearinghouse services will pay the Clearinghouse directly, as relevant. The pricing model is to be worked out with the Clearinghouse service provider and more detail will be published as available.