This document has been prepared by ARI Registry Services in consultation with Neustar, Verisign and Demand Media. This document has also been reviewed by the TMCH-Tech working group and is now offered to the broader community for review and comment.

Should you have any questions or comments about this document please send an email to:

- Chris Wright, Chief Technology Officer at ARI Registry Services - chris.wright@ariservices.com, or
- Post to the ICANN TMCH-Tech working group - to post a message to all the list members, send email to tmch-tech@icann.org.

1 Proposed model for trademark claims

The following proposed model is offered for trademark claims, improving the proposed ICANN model while meeting all requirements set forth in the Applicant Guidebook.

This proposed model simplifies the ICANN model by separating the claims process in to two key questions:

1. Does a claim exist for this DNS label?; and
2. Give me the claims notice for this DNS label.

This keeps the bulk of the data centralized at the Trademark Clearinghouse (TMCH).

2 Details of the proposed model

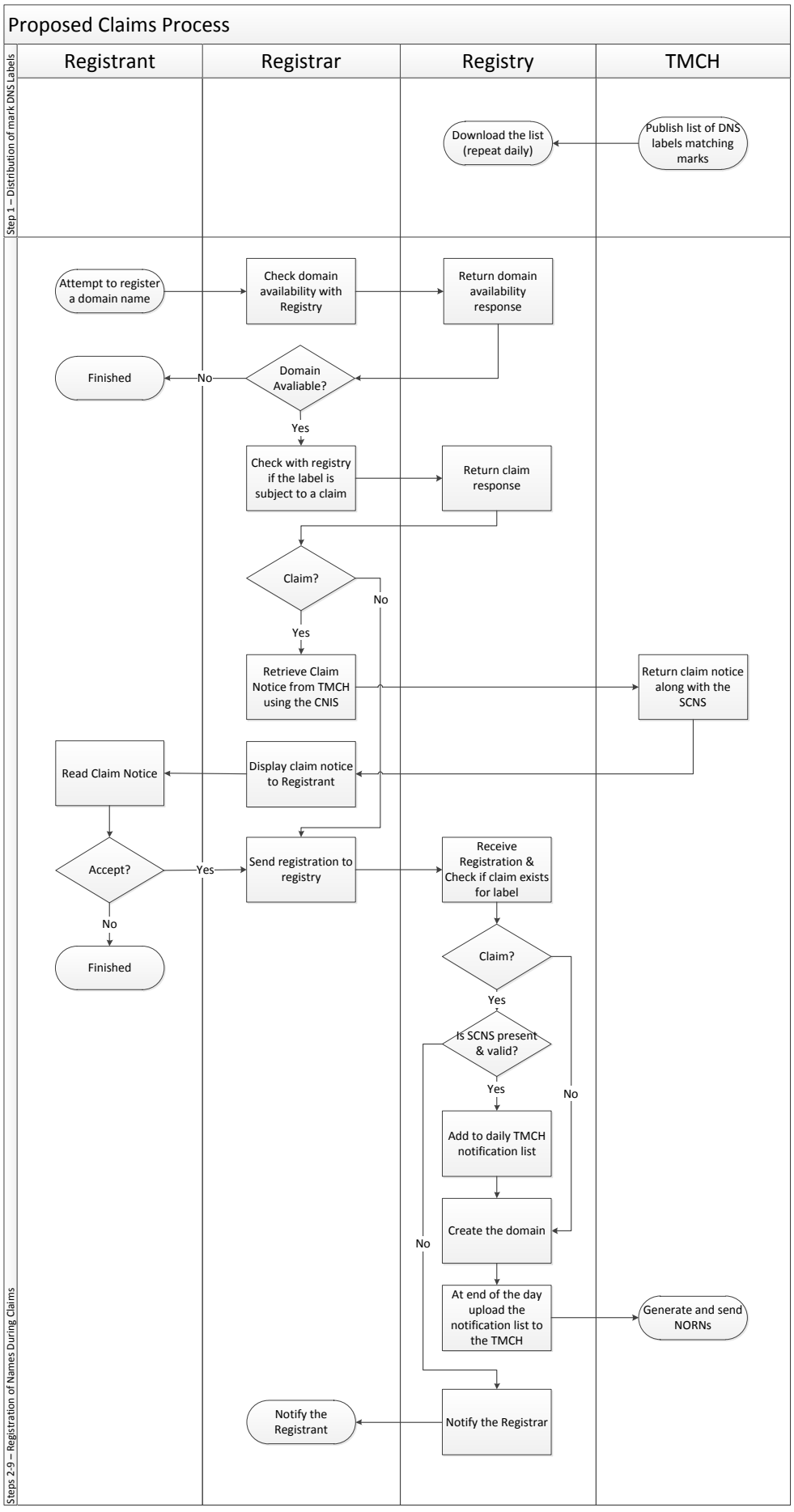
The steps of operation of the proposed model are as follows:

1. The TMCH periodically publishes a list of DNS labels that are known to match trademarks registered in the clearinghouse (see publishing the list below in section 3.1). This list includes a random unique string that is assigned to the label. Registries can download this list and use it in their registration systems to answer question 1 above.
2. A potential registrant approaches a registrar to register a domain name (or submit an application for a domain name).
3. The registrar checks if the name is available using the normal EPP Check mechanism (if this is applicable). The registrar can continue to do all the normal value adds they may offer such as ‘name spinners’ or the like.
4. Once the registrant has identified the name they would like the registrar then uses a new EPP command (to be standardized as part of the EPP extension – this is further discussed in section 4) to check with the registry if the domain name matches a claimed mark. The registry will check to see if the label is present on the list of marks downloaded in step 1.
    a. If there is a match the registry returns the unique string to the registrar and this process continues, otherwise
    b. The registration/application continues as normal for that TLD and we move to step 8.

5. The registrar now has access to the unique string that they will need to use in the HTTP query below.
    a. The registrar then obtains the claims notice content from the Claims Notice Info Service (CNIS) using the HTTP protocol (which is further discussed in section 3.2). As part of getting this information the registrar provides the unique string obtained from the step 4.a. as well as the complete domain name being registered/applied for.
    b. The CNIS returns the claims notice information accompanied with a Signed Claims Notice Signature (SCNS) that is digitally signed using the TMCH private key. The SCNS (further described in section 3.4) includes a timestamp of when it was generated, a validity period, and the domain name used in the CNIS request which is all digitally signed using an XML signature. The SCNS can be used by the registrar with a subsequent domain create command and then can be validated by the registry.
6. The registrant reads and accepts the claim notice.
7. The registrar then sends the create command to the registry to create the domain name. This command will include the SCNS that must have been obtained from the TMCH. This command will also include the details of who accepted the notice (the client IP address) and a timestamp of when the notice was accepted.
8. The registry verifies whether or not the DNS label is subject to a claim and that, if so, an SCNS is present.
    a. If an SCNS is not required, the domain name is registered as normal, otherwise
    b. The SCNS is validated using the TMCH's public key and the information within is cross checked with the domain name being created. If matching the registration succeeds, if not it fails. The registry records the SCNS identifier included in the SCNS along with the client IP address and acceptance timestamp.
9. The registry notifies the TMCH of the registered domain names for the purpose of notifying mark holders about the fact that a domain name was registered that matches their mark as well as reporting purposes. These notices will be referred to as 'Notification Of Registered Name' notices (NORN) and is described in 3.5. This notice should include the identifier from the SCNS. This combination of the domain name and the SCNS identifier can be used to trace the claims notice end-to-end (TMCH to Registrar to Registry to TMCH). A daily upload of registered domain names to the TMCH is sufficient for this purpose.

This proposed solution works for those that are conducting 'first come, first served' or landrush style processes.

These steps are illustrated in the following diagram:


Proposed Claims Process
Registrant
Registrar
Registry
TMCH
Step 1 – Distribution of mark DNS Labels
Steps 2-9 – Registration of Names During Claims
Download the list (repeat daily)
Publish list of DNS labels matching marks
Attempt to register a domain name
Check domain availability with Registry
Return domain availability response
Finished
No
Domain Avaliable?
Yes
Check with registry if the label is subject to a claim
Return claim response
Claim?
No
Yes
Retrieve Claim Notice from TMCH using the CNIS
Return claim notice along with the SCNS
Read Claim Notice
Display claim notice to Registrant
Accept?
Yes
Send registration to registry
Receive Registration & Check if claim exists for label
No
Finished
Claim?
Yes
Is SCNS present & valid?
Yes
No
Add to daily TMCH notification list
Create the domain
No
At end of the day upload the notification list to the TMCH
Generate and send NORNs
Notify the Registrant
Notify the Registrar

3 The model in detail

We will now examine this model in more detail.

3.1 Publishing the list of marks

Given that the TMCH has already deduced the list of marks and the labels that represent those marks, publishing that list is relatively trivial. The choice of HTTP makes sense as all the TMCH needs to do is provide the list, preferably compressed, and allow registries to download it at will. Registries should be required to download the latest list at least once a day but may do it more frequently if they desire.

This means that at most there will be a 24 hour lag between someone being approved in the TMCH and the mark being protected. Given the highly compressible nature of text files, it is considered that writing the logic at both ends to generate and apply differentials is unnecessary effort and that simply re-downloading the entire list should be a relatively easy task.

The list should be a 7 bit ASCII clean CSV and include the following fields:

- The DNS label used to compare to the label sought for registration; and
- The random unique string needed to retrieve the claims notice from the TMCH.

3.2 The Claims Notice Info Service (CNIS)

When a claim is matched against the list and the unique code is returned to the registrar, the registrar now has all the information it requires to construct a URL to retrieve the claim notice from the CNIS, e.g.:

http://claimsnotice.tmch.icann.org/claims/generatNotice?domain=<domain-name>&randomCode=<code-from-list>

This URL will be for a simple ‘rest like’ web service. The TMCH would then return the claim notice and the SCNS in XML format, which the registrar can frame or use ‘AJAX like’ practices to present to the potential registrant.

Contained within the response will be a Signed Claim Notice Signature (SCNS) unique to that claims notice which must be returned to the registry.

3.3 The use of PKI

This model proposes the use of a PKI style, public key pair. In simple terms PKI enables one party to digitally sign some information using a private key which is known only to them, and then other parties can verify the signature on the information utilizing the public key which is known to all. If any of the information is changed after it is signed or if the signature has been generated using a private key that does not correspond to the public key, then verification will fail. In this case, the information signed and the digital signature is referred to as a Signed Claim Notice Signature (SCNS).

By using PKI technology the TMCH only need to make available a public-key. The registry still has the responsibility of validating that the claims notice was presented during domain name registration. The registry can validate the domain name included in the SCNS and record the unique identifier for auditing and traceability back to the TMCH.

It is important to note that the claims information of the notice is not signed by the TMCH or passed to the registry at all, which helps to reduce the exposure of the information. The registry validates the signature of the SCNS using the TMCH public-key.

Using PKI enables the TMCH to be decoupled with the registrars and registries since there are no direct interface dependencies between the parties to fulfill the verification of claims notice requirement. The decoupling of the TMCH and the registry systems simplifies the overall system.

Due to the use of PKI, we need to deal with one scenario related to security.

Scenario 1: Compromise of the TMCH public/private key pair

In this highly unlikely scenario we are discussing what would happen if the TMCH did not adequately protect the private key, such that it becomes compromised in some way.

If this were to occur, the action to take is relatively simple. The TMCH need only notify all the Registries that the current public key is no longer valid, and issue a new public key.

3.4 The Signed Claim Notice Signature (SCNS) data

The information to be included in the Signed Claim Notice Signature (SCNS) data is expected to be the following:

- A SCNS Identifier that is a unique identifier generated by the TMCH for each notice requested from the CNIS
  This identifier uniquely identifies the notice data for support and matching purposes;
- A timestamp of when the information was generated and signed
  This enables a registry to tell when the claims notice was generated (and viewed) with respect to when the actual command was sent to the registry, it also prevents reuse of signed claims data ensuring that the notice was specific for this domain name registration;
- The fully qualified domain name that the SCNS is for
  This prevents reuse of SCNS ensuring that the notice was specific for this domain registration; and
- A digital signature generated over all the SCNS data using the TMCH private key.
  Verifies that the claim notice data was created by the CNIS for that registration.

This information should be sent to the registrar as part of requesting the claims notice. The data should be an XML string utilizing UTF8 encoding. This string is human readable, and can easily be understood by engineers and support personnel when investigating problems.

3.5 Notification of Registered Name (NORN) notices

By periodically uploading to the clearinghouse a file indicating registrations/applications that have taken place with a claims notice (i.e. SCNS passed to registry in the domain create), the TMCH can identify the relevant mark holders and notify them (and anyone else) as appropriate.

This information can also be used for reporting purposes and will be useful in evaluating the success of the program.

The file should be a UTF8 encoded text file with a simple format (e.g. CSV), the fields of which are:

- SCNS identifier
  To allow matching of registration to notices;
- Domain name
  To allow reference to the domain name in notifications to other mark holders; and

- Creation timestamp
  To be included in the notice to other mark holders, also to assist with duplicate detection and to help with temporal issues.

The registry would send the simple file daily to the TMCH utilizing a HTTP, SFTP or SCP over SSH upload.

4 The benefits of the proposed model

There are a number of benefits to this approach; some of these have been explored below. The proposed model:

- Protects mark information against data mining – this solution provides the best protection possible as:
  - The URLs for claims notices are not predictable,
  - The TMCH can see all requests for claims notices and can monitor, rate limit or whatever else it deems necessary to protect the data, and
  - Data is centralized only at the TMCH, so all access is known and controlled by them,
- Allows registrars (the entities with the customer relationship) to provide feedback to potential registrants immediately, especially when checking domain names across multiple TLDs,
- Is technically efficient and very simple to implement, and
- Is auditable, as having the registrar obtain a signature from the TMCH, then making the registrant read and accept the notice from the registrars site, then sending this signature to the registry, then finally the registry sending it full circle back to the clearinghouse and enforcing each party to do these things contractually provides a clearly auditable chain of events that if later can be used to prove that notices where generated, and viewed by the registrant.

Finally, another benefit is that one simplified standardized EPP extension will be produced to allow this 'signed claim data' to be transmitted to the registry;. Work has already started on defining this EPP extension.

5 Requirements of this model for the TMCH

This proposed model places technical requirements on the TMCH to provision claims notices over a HTTP based web service. The provision of this simple (web) service does not differ greatly from the provision of the mark registration and validation service they will already need to supply. However the ICANN requirements currently impose that registrations cannot proceed unless relevant claims notices have been presented and accepted. This places the ability of a domain name to be registered within the hands of the TMCH.

Due to the fact that we have separated the question of whether or not there is a claim for a domain name (which we have made 100% available), and what is the claim information, we are prepared to accept that during periods of TMCH down time, only registrations for that do not have a claim can proceed.

We are willing to accept this situation if the TMCH provider is held to strict requirements in the provisioning of this service. These requirements should be in line with those standards that registry operators must meet and should include things such as:

- The data should be escrowed to a reputable escrow provider and the BCP requirements of the system should be considered;
- Robustness of the system should be commensurate with those that domain name registries need to meet including that the CNIS should be provided from at least two independent locations with data replicated between the two sites;
- Strict SLAs on the availability and performance of the services;
- Financial penalties payable to both registries and registrars on breach of SLAs; and
- The financial penalty mentioned above is important as it ensures that the TMCH takes the system seriously and motivates them to invest appropriate resources into quality development, systems and testing.

6 Outstanding issues

There are a number of outstanding issues that affect all claims models that still need community discussion. These include:

- How long after retrieving a notice is it allowed to be accepted for use in a domain name registration?
- How long after viewing and accepting a notice is that acceptance allowed to be used in a domain registration without checking for updated data at the TMCH?
- How are claims to work during landrush style period where registrations are not on a first-come, first served principal?
- How are we to deal with pre-registrations?

7 How this addresses our concerns

The document *TMCH - Issues with the ICANN Proposed Model - 1.0* describes issues with the current proposed solution put forward by ICANN. Each of those issues is explored below with explanation as to how the proposed solution addresses those issues.

1. Unnecessary and obscure encryption, with no relation to the actual domain label they represent, make diagnosing errors and providing customer support difficult for both Registries and Registrars
   By including human readable details in the 'signed claim data' and eliminating the 'encryption' (or the need for encryption) in all other parts, the ability to support domain registrants (and registrars) is significantly increased;
2. The TMCH Outage problem
   This solution suggests that we can deal with the outage problem if the availability of the marks DNS label list if dealt with;
3. The ICANN model currently calls for distributing the entire TMCH database of trademarks to domain name registries during the Trademark Claims Service Period
   This proposal presents an inherently more secure design where the TMCH manages the data in as a single authoritative source where security can be centrally managed - the

TMCH would be able to rate limit and protect against abusive entities attempting to mine the data for unknown purposes;

4. The burden for Registries to have to protect and securely manage trademark data
   This model does not replicate the entire data set to registries or registrars thus these issues (including the associated indemnifications) do not exist – a simple list of DNS labels is all that is shared in this proposal;
5. The unnecessary burden placed on the TMCH and Registries to replicate data for every entry in the clearinghouse even though only a small percentage of those marks will match names registered during the claims period (first 60 days – for most)
   By allowing the clearinghouse to only generate 'signed data' on demand, and by using PKI we eliminate unnecessary code generation and we only need to replicate the list of DNS labels covered by marks data to other parties, then registries only need a public key which can be provided 100% publically – both the public key and the DNS label list can be implemented using a simple 'pull' model; and
6. The unnecessary burden of replicating data to all the different registries when there are alternative models that meet all the objectives of all parties and don't suffer from any of the issues raised here without requiring replication of TMCH database data
   Same reason as above.

8 Conclusion

This solution meets all of the goals of the program using mechanisms that greatly simplify the process of registering a domain name during sunrise.

By simplifying the process we are making it easier for registries and registrars to provide IP holders with the protections afforded to them under the trademark claims program. A simple process reduces the chance for error and takes overall costs out of the ecosystem.