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.

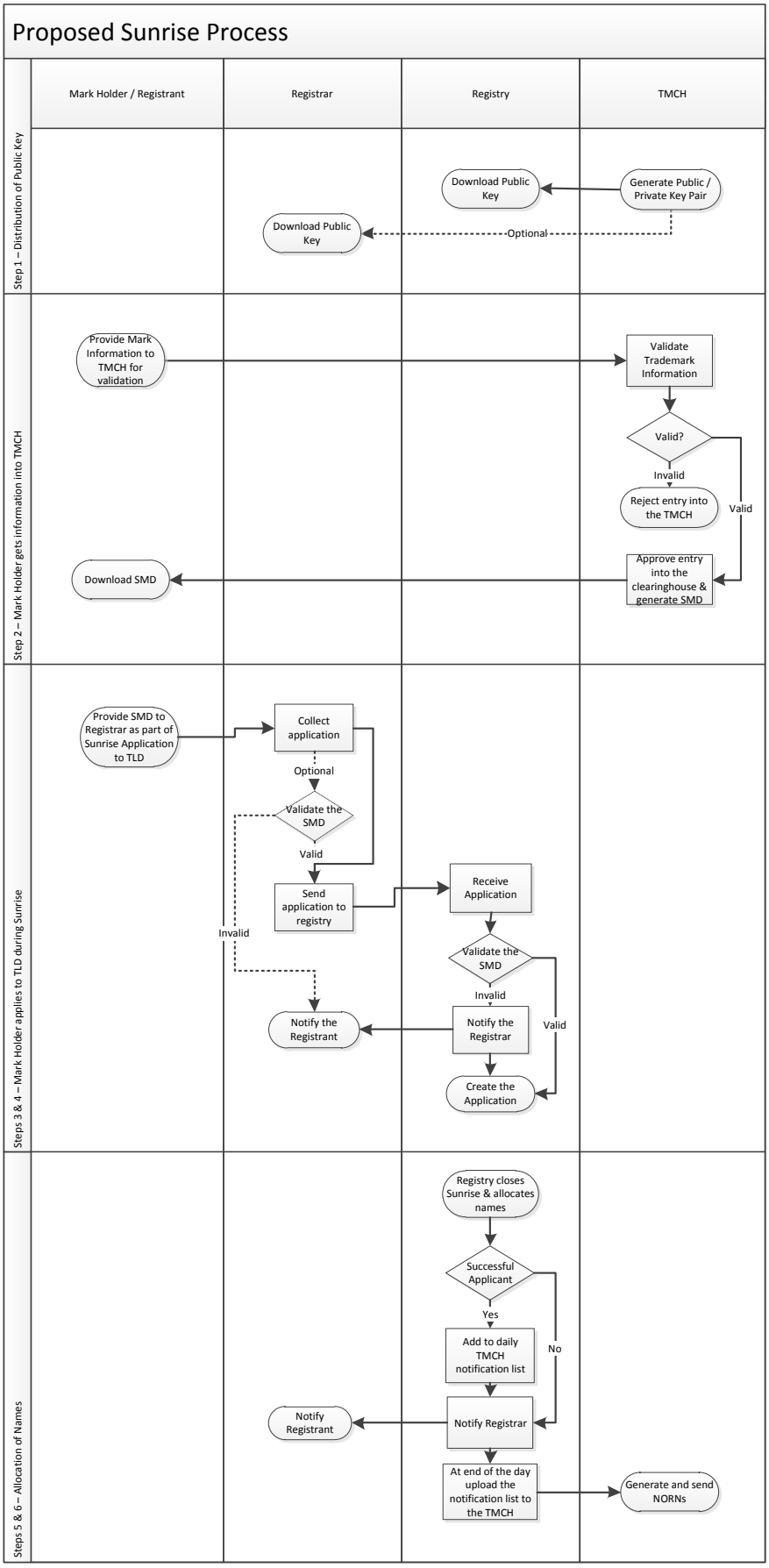
1 Proposed model for sunrise

The following proposed model is offered for sunrise, improving the proposed ICANN model while meeting all requirements set forth in the Applicant Guidebook. This proposed model simplifies the ICANN model by decreasing the coupling between the Trademark Clearinghouse (TMCH) and registries. The model is as follows:

1. The TMCH generates and maintains a global public-private key pair and provides the public key to the registrars and registries. This can be done simply by publishing the public key on the TMCH website. This website should be provided over HTTPs using a digital certificate from a reputable certificate authority. The DNS records associated with this website should be protected using DNSSEC. We believe that there are no issues with security of the public key and anyone in the world can have access to it.
2. Once the TMCH has authenticated the trademark information provided by the trademark holder, and validated the use requirements for eligibility to participate in sunrise, the TMCH signs the sunrise (trademark) data with its private key. The digitally signed information is referred to as the 'Signed Mark Data' (SMD) and is provided to the mark holder. Typically, this would be in the form of a file download from the TMCH website. The SMD includes all of the domain labels (domain names) possible to be used in registrations for the validated trademark (IDN variants excluded).
3. As each TLD begins its sunrise phase, the mark holder selects a registrar and provides the registrar with the SMD as part of an application for a name within the applicable sunrise period. The registrar (or its reseller) has the ability, if it chooses to, to validate the information using the TMCH public key and then forward the information to the registry to create the application.
4. The registry verifies the signature of the SMD with the public key and verifies that one of the labels within the SMD matches the domain label being registered. The registry may also then verify any other information in the SMD to ensure it is consistent with the registry's sunrise eligibility policies. The application, or domain name, is then created.
5. At the closure of the sunrise round, the registry operator will then make allocations of domain names.
6. The registry notifies the TMCH of the registered domain names for the purpose of notifying mark holders about the fact that a 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). We believe that a daily upload of registered names to the TMCH is sufficient for the purpose of generating NORN notices.

This solution also works for those that are conducting 'first come – first served' style sunrise processes.

These steps are illustrated in the following diagram:



2 The model in detail

We will now examine this model in more detail.

2.1 The use of PKI

This model proposes the use of a PKI style, public / private 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.

By using PKI technology the TMCH only need make available a public-key. Whilst registrars can us this public key to pre-validate the signature on mark information (see below)the registry still has the ultimate responsibility of ensuring mark registration data is valid during domain name registration. Verifying the digital signature on the SMD using the TMCH public-key asserts the necessary validity of the data. The registry can apply any additional sunrise eligibility requirements using the SMD information, which can be trusted based on its digital signature.

Using PKI enables the TMCH to be decoupled from registrars and registries since there are no direct interface dependencies between the parties to fulfill the sunrise application flow. The decoupling of the TMCH and registry systems simplifies the overall structure and allows the support of scenarios when the sunrise period is changed or extended, and provides for participants that were not present in the TMCH at commencement of sunrise to participate in the sunrise by having their marks authenticated and validated prior to the expiration of the applicable sunrise periods.

Further, registrars may use the public key to pre-verify data before it is submitted to the registry, enabling them to notify the customer and correct the issue immediately. Registrars are in the best position to do this because they ultimately own and manage the relationship with the customer (registrant).

2.2 PKI and security

Due to the use of PKI, we need to deal with three scenarios related to security. These are detailed as follows.

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

In this highly unlikely scenario we discuss 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.

Any registry receiving requests utilizing data signed with the old key, would reject the requests and instruct registrants (via registrars) to return to the TMCH to obtain updated signed data. Registrars could verify this before the command is even sent to the Registry.

The likelihood of this happening is extremely low and the fix relatively simple to implement. Only those trying to register domain names using keys provided before the compromise will be affected, and it will be relatively simple for them to obtain newly signed data.

2.2.2 Scenario 2: Mistakes in signed data

In this scenario we consider the unlikely situation where the TMCH verifies a trademark and generates the signed data, only later to discover that, for one reason or another, the signed information is incorrect. In this situation, the TMCH needs to 'revoke' the signed data, and communicate this fact to registries (and other parties) so that they now know not to accept sunrise registrations using this signed data.

This can be facilitated using a mechanism that is similar to what is more commonly referred to as a Certificate Revocation List for digital certificates. The TMCH will simply publish a list of the 'serial numbers' of signed data that has been revoked; this is referred to as the 'SMD Revocation List'.

It is expected that this list will be small, as the number of mistakes is expected to be very small. This list will be signed by the TMCH and available for download by the registries. The registries will compare the serial number included in a SMD with the SMD Revocation List during the sunrise application flow. Registries will be required to download the SMD Revocation List daily basis and ensure that they do not accept any SMD appearing on the SMD Revocation List. This is not considered a burdensome or problematic process.

2.2.3 Scenario 3: Compromise of an entities signed data

In this scenario we consider the situation where entities signed data that it has received from the TMCH is compromised in some fashion (typically meaning the entities signed data has been obtained by another party).

In this instance the signed data could be revoked as described in Scenario 2. However, if the Registrant information is embedded in the signed data as described in Section 2.3, this is potentially unnecessary. The effect that another entity having this signed data will have would be the ability to register a domain name to the registrant listed in the signed data, effectively registering the domain name for someone else – what purpose could this serve? Additionally if they did, the actual registrant (owner of the mark) would be entitled to the domain name. The actual owner would be notified of the registration though the notification mechanism already built into the RPMs and thus is completely protected against the situation. Even if we decide that the overall solution should have a mechanism that allows compromised client signed data to be revoked, the situation can still exist where the mark holders signed data is exposed without their knowledge, and thus they cannot apply to have it revoked.

We do not foresee this as an issue for a number of reasons, firstly the mark holder is completely in control of their own destiny, as it is their data to protect, and secondly this issue already exists with the ICANN proposed model.

2.3 The Signed Mark Data (SMD) file

The information to be included in the SMD file is expected to be the following:

- A serial number
  To uniquely identify the data for support and revocation purposes;
- A validity period for the information
  To enforce that the data be 'renewed' with the clearinghouse each year;
- The label(s) that the mark covers
  So that the TMCH can enforce consistent rules for normalizing a mark to a domain label (this is not intended to cover IDN variants);

- Trademark Information (including: the mark name, the registration date of the mark and other information such as jurisdiction and class – exact fields to be discussed with representatives of mark holders and registries alike)
  To be used for allocation purposes, extended eligibility checks and display of certain fields in the WHOIS;
- Owner information – such as organization name and address, (these would be based on the EPP contact fields)
  Could be used as the registrant contact in any domain name registration (or application) applied for using this signed data; and
- A digital signature generated over all the data using the TMCH private key
  To enable digital verification that all the information is accurate and as validated by the TMCH.

This signed data should be downloaded by the mark holder as a file. This file should be an XML based file utilizing UTF8 encoding. The file is human readable, and can easily be understood by mark holders, especially those juggling many different files for many trademarks.

Support staff at resellers, registrars and registries when assisting with support issues can also easily understand these files. In fact the file can even be displayed in a web browser, and by referencing an external XLST, can be formatted into a human friendly table like structure.

2.4 Notification of Registered Name (NORN) notices

By periodically uploading a file indicating sunrise registrations that have taken place, 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:

1. Serial number
   To allow the TMCH to detect previously undetected signed data (or key) compromises;
2. Domain name
   To allow reference to the domain name in notifications to other mark holders; and
3. Creation timestamp
   To be included in the notice to all 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. Registries should be required to continually retry unsuccessful uploads until they are successful.

3 The benefits of the proposed model

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

3.1 Reduced complexity

Some registries will ultimately need verified trademark data during the sunrise process. In the past each TLD launch would ask for all the information and supporting evidence from the

mark holder, charge a large fee to have the information verified and then use it in their processes. In this model the data is validated once by the TMCH then returned to the mark holder, who then voluntarily gives it to each TLD for which they wish to participate in the sunrise.

The registry then simply validates that the signature is valid for the data supplied and, if valid, knows the data has been unmodified and has been independently verified by the trademark clearing house thus does not have to verify it themselves. The mark holder is only required to provide a single SMD instead of having to re-enter the trademark information on a per TLD basis to satisfy the registry sunrise eligibility requirements. Cost and complexity to the mark holders is significantly reduced.

3.2 Simplified, standardized EPP extension

Another benefit is that one simplified standardized EPP extension needs to be produced to allow this 'signed data' to be transmitted to the registry; no complex check extensions are required. Work has already started on defining this EPP extension.

The latest version of the existing work on this extension can be found at the following link:

http://tools.ietf.org/html/draft-tan-epp-launchphase

By including the registrant contact information within the code, organizations that manage many trademarks, may be able to streamline the registration/application process by using Registrars that enable the upload of zip files containing multiple sunrise files. Other Registrars may be able to simplify the overall process to potential registrants participating in multiple sunrises by allowing them to associate the uploaded SMD with their 'account' once, and then use the data for each sunrise application/registration made by the account.

In addition, by including all the labels that are considered a match for the mark, registrars will be able to streamline the registration process such that mark holders upload only the sunrise code and select the names (where there are multiple labels) for registration. Because the SMD is not obfuscated and contains all the information associated with the signature, registrars (and registries) will be able to identify many issues early, such as malformed input, domain labels not matching the mark, registration date following the cutoff date, incorrect signatures etc. This is critical in supporting users through the sunrise process.

3.3 Additional uses for SMD information

The information available in the SMD may be used to supplement responses to WHOIS queries, providing visibility into the mark that was used to establish eligibility. As the entity that owns the mark has voluntarily submitted the information to the registry, they have remained in full control of their own private data. As they have elected to submit the data to the registry, there are no privacy issues with this approach.

Another benefit of the TMCH creating the SMD is that, independent of the sunrise process, URS providers can request SMD from mark holders making URS claims based on information they have in the clearing house. This way URS providers can know they have received validated information, without requiring the URS provider to integrate with the TMCH (they need only verify the SMD with the public key as per registries and registrars).

3.4 Other benefits

This solution is highly available and allows for TMCH down time, due to the decoupled nature of its design. The ability to verify SMDs is independent of the availability of the TMCH system.

In this model the only two people who have access to trademark information are the TMCH and mark holders themselves. Only if a mark holder voluntarily gives the information to a registry (via a registrar) during a sunrise process do other parties get access to that information. Over all this solution is simple and that ultimately reduces cost for all parties involved.

4 How this addresses our concerns

The document *TMCH - Issues with the ICANN Proposed Model - 1.0* describes issues with the currently 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. Inability to participate in a sunrise if you are not in the clearinghouse prior to the start of that sunrise
   By allowing the TMCH to use PKI technology to signed trademark data at any point in time which can be verified by the TMCH public key this issue is eliminated;
2. Unique codes per trademark/registry combination put unnecessary burden on trademark owners
   By requiring only one file of 'signed data' for each mark in the clearinghouse the number of 'codes' that mark holders need to deal with is greatly reduced. Combine this with smarter registrars enabling the SMD to be uploaded once and reused over and over the process is significantly simplified for mark owners (or their agents);
3. Obscure codes, with no relation to the actual domain label they represent, make diagnosing errors and providing customer support difficult for both Registries and Registrars to do
   By including human readable details in the SMD the ability to support mark holders and their agents is significantly increased. The internal management of codes for multiple trademarks is also greatly simplified;
4. No access to trademark information for registries, meaning its unable to be used in applying further eligibility rules, for hierarchical allocation models or displayed in the WHOIS - meaning Registries will need to independently request and re-validate trademark information increasing costs for sunrise registrations
   By including the data in the SMD this allows registries to get access to the information they need, by providing this SMD to the mark holder, mark holders are in full control of their own data and choose whom they give it to, and whom they don't;
5. The unnecessary burden placed on the:
   - TMCH to generate codes for; and
   - Registries to replicate codes for

   every eligible (for some definition of eligible) mark in the clearinghouse even though only a small percentage of those marks will participate in each sunrise
   By allowing the clearinghouse to only generate 'signed data' on demand, and by using PKI we eliminate unnecessary code generation and we don't need to replicate any data to any other parties, only a public key and revocation list is needed to be provided, both which can be provided 100% publically and can be implemented using a '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 as point 5.

5 Conclusion

We believe that 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 mark holders to apply for and manage their portfolio of applications and registrations. A simple process reduces the chance for error and takes overall costs out of the ecosystem.