New gTLD Transfer Process

v.02 CPH TechOps Discussion Paper

1. Abstract

Changes in the WHOIS system resulted from the GDPR legislation that went into effect on 26 May 2018. These changes impacted the ability for ICANN Accredited Registrars to facilitate the process of inter-registrar domain name transfers, as the WHOIS, prior to GDPR, played a critical role in validation and communication steps that had been in place to meet certain compliance requirements while ensuring reliable and reasonable confirmation of the transfer and parties involved. With WHOIS changing, the gTLD registrar transfer process and compliance requirements from ICANN that registrars must meet required modification in order to preserve the overall inter-registrar transfer functionality..

After an in-depth discussion, the Contracted Party House (CPH) TechOps group ("CPH TechOps") reviewed the impacts, and suggested an interim solution[1] on 1 May 2018 which was included into the Temporary Specification for gTLD registration data[2] as Annex G, issued 17 May 2018.

Since the Temporary Specification supersedes all other relevant ICANN policies in regard to transfers, Annex G now governs the gTLD transfer process for the duration of the Temporary Specification, which can be upheld for a maximum of 12 months.

At the GDD Summit[3] in Vancouver in May 2018, the CPH TechOps group convened two workshops to explore what a new transfer policy could look like in light of the GDPR.

Though no final transfer process was developed, the attendees agreed on a set of high-level principles that should guide the further discussion.

These principles are:

---

[1] https://www.icann.org/en/system/files/correspondence/sattler-to-atallah-01may18-en.pdf
[2] https://www.icann.org/resources/pages/gtld-registration-data-specs-en
[3] https://www.icann.org/gddsummit

- The transfer process must comply with current data privacy regulations
- The transfer process must be instant, however a time to validate the legitimacy of transfer should be given
- A transfer token shall be sufficient to authorize a transfer
- No personal data shall be transferred from the old to the new Registrar
- The existing gTLD transfer policy should be changed as little as possible

At ICANN 63[4] in Barcelona,October 2018 the CPH TechOps group held a workshop based on the discussion of the "New gTLD Transfer Process CPH Discussion Paper v.01"[5]. Four topics were worked upon in detail:

1. **Who is responsible for Transfer Token & TTL handling/storage/processing — Registrar/Registry/both?**

   Since the Transfer Token/AuthCode and the corresponding TTL are the central elements in the proposed new transfer process it was concluded that, to reach a uniform, transparent, and predictable process, Registries should be in control of the storage and processing of the AuthCode, regarding the technical part. To be able to roll this security policy implementation out to all Registries and Registrars there could be a very narrow (fast track) policy process rendering the technical flow into binding policy.

   It was also concluded that, while the policy process and implementation of such is underway, the Transfer Token/AuthCode should be set by the Registrar according to a to-be-developed best practice.

   This provisional behaviour will be outlined below in addition to the new process, and shall cease to exist once the new policy is implemented.

2. **Should the transfer check of the Losing Registrar be mandatory or optional?**

[4] https://meetings.icann.org/en/barcelona63
[5] New gTLD Transfer Process CPH Discussion Paper v.01

The group agreed that the requirement to notify the Registrant about a transfer request should be mandatory. As general business practises of Registrars and individual transfer scenarios vary, the group concluded that such notification does not have to be an email, but rather may incorporate other means of more modern communication.

To increase security the group suggest that only the registrant should be able to request a transfer; this would eliminate the admin contact acting as another party who is able to approve or request transfers.

3. **Do we need a process in case the Losing Registrar is not responding? Should there be a ccTLD-like Registry involvement?**

   Due to the importance of the cooperation of the Losing Registrar in a Transfer scenario the group was unanimously in favor of having such a process.

   After deliberating in depth about the possibilities of a ccTLD-like Registry involvement, it was found that because of potential GDPR restrictions as well as legal and language reasons a gTLD Registry would very likely not be able to perform such service in a manner satisfying for all parties.

   As the expected behavior of the Losing Registrar is mandated by ICANN policy the lack of responsiveness constitutes a deviation from such and should hence be dealt with via an ICANN Compliance Process.

   To discourage premature/frivolous compliance requests which may pose an extraordinary burden on the ICANN Compliance team it was concluded that only the Gaining Registrar should be able to invoke such a process. It was also agreed that before opening a case the Gaining Registrar must try to resolve the issue with the Losing Registrar via the TEAC directly

4. **Possible values for the TTL i.e 1 to 15 days or 1 hour to 30 days …. Do we need a policy/best practice about the syntax of a transfer token (length, characters)? Should we use the term transfer token or AuthCode, do we need a definition?**

The group was in agreement that the term describing the transfer password should be AuthCode, as this term is already in use and well known. It was also agreed that there must be a policy to manage the syntax of the AuthCode as well as the allowed values of the TTL.

In regard to the TTL the group suggested a validity of no more than 14 days, presented as the total number of hours until TTL expiration. There was no resolution for a minimum TTL requirement, because registrars with different business models may have different requirements for how quickly a domain name gets unlocked and transferred.

More work on any of these topics is needed.

To advance the discussion, the following text describes a new transfer process in adherence to the high-level principles and findings of the workshop.

2. Overview

The gTLD Registrar transfer process can be divided into three distinct phases:

1. Registrant initiates domain name transfer process with Losing Registrar
2. Registrant requests domain name transfer with Gaining Registrar
3. Registry transfers domain name from Losing Registrar to Gaining Registrar

For each of the phases, every involved party has to adhere to a defined set of policies and technical transactions.

3. Transfer Phases

3.1. Registrant initiates domain name transfer

Flow

- Registrant requests issuance of an AuthCode from Losing Registrar
- Losing Registrar verifies AuthCode request

- Losing Registrar checks Client Transfer Lock
- Losing Registar checks Server Transfer Lock
- Losing Registrar verifies no applicable Registrant changes within last 60 days
- If no Transfer Lock is set AuthCode request proceeds
- Losing Registrar sets AuthCode & TTL via EPP in Registry system
- Losing Registrar communicates AuthCode & TTL to the registrant

Policy

The Losing Registrar MUST verify the authenticity of the AuthCode request according to their internal policies and practices (which may vary depending on the business model). This MUST involve a notification to the current registrant contact[6] through a medium (email, phone, messenger, etc.) of the Registrar's choosing sent at the time when the request is made. Once those required steps are completed, the AuthCode must be issued to the requestor within five days of the request, unless there is an explicit request by the registrant or requestor to cancel the process, or the request verification was not successful.

Technical

On request and after verification, the Losing Registrar generates an AuthCode following best practices[7] and submits the AuthCode & TTL via EPP to the Registry System.

TTL : TBD (Best practise to be established)
EPP : <domain:update>

Until Registries have incorporated the TTL function into the protocol and their Registry Systems the Registrar should be responsible for setting a TTL in its own system adherence to a to-be-developed best practice.

[6] https://www.icann.org/resources/pages/foa-registrar-transfer-confirmation-2016-06-01-en

[7] To be defined

Changes to standard

- New verification/notification requirement before issuance of AuthCode by Losing Registrar. No FOA2.
- A TTL is set for each Authcode in Registry System

Additional related steps not part of this process/policy

- Registrant removes transfer lock (if applicable)

3.2. Registrant authorizes domain name transfer

Flow

- Registrant orders domain name transfer with Gaining Registrar
- Registrant submits AuthCode to Gaining Registrar
- Gaining Registrar submits transfer request via EPP to Registry System
- Registry Operator checks and acknowledges transaction

Policy

Receiving an AuthCode is sufficient for the Gaining Registrar to initiate a transfer request.

Technical

Using standard EPP Transfer domain routine

EPP : <domain:transfer>
Syntax : as defined in RFC5731

Changes to standard

- No FOA1 Process for Gaining Registrar

3.3. Registry transfers the domain name

Flow

- Registry Operator checks Client Transfer Lock
- Registry Operator checks Server Transfer Lock
- Registry Operator checks AuthCode
- Registry Operator checks TTL
- Registry Operator notifies Gaining Registrar of transfer failure in case any check fails
- Registry Operator transfers domain object to Gaining Registrar
- Registry Operator notifies Gaining Registrar of transfer success in case no check fails
- Registry Operator notifies Losing Registrar of transfer success in case no check fails
- Registry Operator notifies Gaining Registrar of transfer of domain object
- Gaining Registrar updates domain object with new registrant data
- Gaining Registrar updates domain object with a new AuthCode, and sets TTL=Null

Policy

- Registry Operator needs to adhere to existing transfer policies[8] regarding lock status
- Registry Operator will transfer domain name immediately
- Registry Operator will not transfer any contact data with the domain object.

Technical

Using standard EPP transfer routine where possible

Until Registries have incorporated the TTL function into the protocol and their Registry Systems, Registries must not check the TTL.

Changes to standard

- Validity of the TTL must be processed
- Transfer must be processed immediately
- Transfer of domain object without contact data

[8] https://www.icann.org/resources/pages/registrars/transfers-en

4. Use cases and expected behavior regarding AuthCode

4.1. Registrant initiates transfer

- Losing Registrar sets new AuthCode & TTL at the Registry
- Losing Registrar informs the Registrant about AuthCode & TTL
- Losing Registrar does not store AuthCode token

4.2. Registrant lost AuthCode

- Losing Registrar sets new AuthCode & TTL at the Registry
- Losing Registrar informs the Registrant about AuthCode & TTL
- Losing Registrar does not store AuthCode

4.3. Registrant cancels transfer

- Losing Registrar updates domain object with a new AuthCode, and sets TTL=Null
- Losing Registrar does not store AuthCode

4.4. Transfer is processed and domain name is transferred to Gaining Registrar

- Registry Operator checks AuthCode & TTL
- Gaining Registrar updates domain object with registrant data
- Gaining Registrar sets new AuthCode and sets TTL=Null at Registry Level
- Gaining Registrar does not store the AuthCode

4.5. Transfer is requested but AuthCode is not correct

- Registry Operator denies the transfer. AuthCode stays as it is.

4.6. TTL of AuthCode expires without transfer being processed

- Registry Operator denies the transfer. AuthCode stays as it is.