AUTH-INFO CODES

INTRODUCTION OF CURRENT APPLICABLE POLICY LANGUAGE

Current Transfer Policy Text re: AuthInfo Codes

- I.5.2 Registrars must provide the Registered Name Holder with the unique "AuthInfo" code and remove the "ClientTransferProhibited" within five (5) calendar days of the Registered Name Holder's initial request if the Registrar does not provide facilities for the Registered Name Holder to generate and manage their own unique "AuthInfo" code and to remove the "ClientTransferProhibited" status.

- I.5.3 Registrars may not employ any mechanism for complying with a Registered Name Holder's request to remove the "ClientTransferProhibited" status or obtain the applicable "AuthInfo Code" that is more restrictive than the mechanisms used for changing any aspect of the Registered Name Holder's contact or name server information.

- I.5.4 The Registrar of Record must not refuse to remove the "ClientTransferProhibited" status or release an "AuthInfo Code" to the Registered Name Holder solely because there is a dispute between the Registered Name Holder and the Registrar over payment.

- I.5.5 Registrar-generated "AuthInfo" codes must be unique on a per-domain basis.

- I.5.6 The "AuthInfo" codes must be used solely to identify a Registered Name Holder, whereas the FOAs still need to be used for authorization or confirmation of a transfer request, as described in Section I.A.2 and Section I.A.4 of this policy.

Commented [1]: I'm interested to know how this is technically accomplished and generated/transferred to the Registry.

Commented [2]: Do we need to account for data processing principles of GDPR?

Current Temp Spec/Interim Reg Data Policy Text re: AuthInfo Codes

- 3. Registrar and Registry Operator SHALL follow best practices in generating and updating the "AuthInfo" code to facilitate a secure transfer process.
- 4. Registry Operator MUST verify that the "AuthInfo" code provided by the Gaining Registrar is valid in order to accept an inter-registrar transfer request.

WORKING DEFINITION

[An Auth-Code (also called an Authorization Code, Auth-Info Code, or transfer code) is a code created by a Registrar to help identify the Registered Name Holder of a domain name in a generic top-level domain (gTLD). An Auth-Code is required for a Registered Name Holder to transfer a domain name from one Registrar to another.] (source)

- Does this definition require updates or changes?

- Can the WG agree on a final form as a candidate for a preliminary draft recommendation that this definition formally exist in the consensus policy?

CHARTER QUESTIONS

RETENTION/OVERALL SECURITY OF AUTH-CODES

b1) Is AuthInfo Code still a secure method for inter-registrar transfers? What evidence was used by the Working Group to make this determination?

Note: In answering this question, the Staff Support Team has added a non-exhaustive list of questions for the WG to consider. Many questions were derived from survey feedback to the Transfer Policy Status Report.

- Some survey respondents noted the AuthInfo Code requires updated security features. Does the Working Group agree? If so, what policy considerations should the group consider? For example, should registrars be required to incorporate a mandatory two-factor authentication requirement or similar added verification layer?
- Should a minimum character limit for the AuthInfo Code be considered? Why or why not?
- Should the auth-code be periodically updated? If so, what policy requirements should be considered?
- Should there be policy requirements around managing the syntax of the AuthInfo Code? If so, why?
- Under what circumstances should the Registrar NOT provide the AuthInfo Code following a request from the registered name holder? If any, should these reasons be considered for a potential policy update?
- What other factors (if any) should be considered regarding the security of the AuthInfo Code?
- What other factors (if any) should be considered regarding the retention of the AuthInfo Code in the inter-registrar transfer process?

AUTHORITATIVE HOLDER OF AUTHINFO CODES

b2) The registrar is currently the authoritative holder of the AuthInfo Code. Should this be maintained, or should the registry be the authoritative AuthInfo Code holder? Why?

Note: As a starting point, the CPH Tech Ops Group concluded "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."

- What does the WG consider to be the advantages (if any) of maintaining the registrar as the authoritative holder of the AuthInfo Code?

- What does the WG consider to be the disadvantages (if any) of maintaining the registrar as the authoritative holder of the AuthInfo Code?
- What does the WG consider to be the advantages (if any) of changing the authoritative holder of the AuthInfo Code to the registry?
- What does the WG consider to be the disadvantages (if any) of changing the authoritative holder of the AuthInfo Code to the registry?

PROVISION OF THE AUTHINFO CODE

b3) The Transfer Policy currently requires registrars to provide the AuthInfo Code to the registrant within five [calendar] days of a request. Is this an appropriate SLA for the registrar's provision of the AuthInfo Code, or does it need to be updated?

Note: The Transfer Policy currently requires the Registrar to provide the AuthInfo Code to the registrant with five calendar days of a request. For reference, the CPH Tech Ops Group chose to retain the five-calendar day SLA.

- Does the WG consider the current five-calendar day SLA a reasonable SLA for provision of the AuthInfo Code? Why or why not?
- Is there any reason to shorten or lengthen the SLA?
- Should the current requirement re: mechanism to transmit the AuthInfo Code remain intact also? [Current requirement provides: I.5.3 Registrars may not employ any mechanism for complying with a Registered Name Holder's request to […] obtain the applicable "AuthInfo Code" that is more restrictive than the mechanisms used for changing any aspect of the Registered Name Holder's contact or name server information"]

EXPIRATION OF THE AUTHINFO CODE

b4) The Transfer Policy does not currently require a standard Time to Live (TTL) for the AuthInfo Code. Should there be a standard Time To Live (TTL) for the AuthInfo Code? In other words, should the AuthInfo Code expire after a certain amount of time (hours, calendar days, etc.)?

As a starting point, the CPH Tech Ops Group concluded "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."

- Should a standard TTL be required for the AuthInfo Code? Why or why not?
- If so, is the TechOps proposal of "no more than 14 days" acceptable to the Working Group? Why or why not?

b5) Should the ability for registrants to request AuthInfo Codes in bulk be streamlined and codified? If so, should additional security measures be considered?

Commented [3]: Maybe instruct/highlight that these can be considered when we get to Topic 5? Or MUST they be addressed here? IF considered, together, this may adjust the project plan.

Note: As a starting point, this charter question was added in response to the following feedback to the Transfer Policy Status Report Survey from the RrSG:[It's] [d]ifficult for Registered Name Holders to retrieve [AuthInfo Codes] for a long list of domains as there are no requirements to permit bulk [AuthCode] requests. (Note: the discussion of partial bulk transfers and the BTAPPA process will be discussed in Phase 2 under question i2. This discussion is limited to the consideration of bulk retrieval of AuthInfo Codes.)

- In light of this concern, should the bulk retrieval of AuthInfo Codes be considered? Why or why not?
- If yes, should additional policy requirements be considered? For example, should an added layer of protection be considered for the provision of more than one AuthInfo Code?

b6) Does the CPH TechOps research provide a logical starting point for future policy work on AuthInfo Codes, or should other options be considered?

Note: As a starting point, the Support Staff Team has included relevant portions of the CPH TechOps paper under the relevant charter questions; however, this does not prevent the WG from considering both the pros and cons of the TechOps suggestions and alternative proposals.

b7) Should required differentiated control panel access also be considered, i.e., the registered name holder is given greater access (including access to the auth code), and additional users, such as web developers would be given lower grade access in order to prevent domain name hijacking?

Note: As a starting point, this charter question was included in response to the following feedback from the Transfer Policy Status Report Survey, "I am concerned about who receive[s] [the AuthCode][.] [I]f we could confirm that only [the] registrant can receive [the AuthCode], then we may no longer need FOA."

- Should differentiated control panel access be a requirement under the Transfer Policy as an added security measure? Why or why not?