Preliminary Recommendations

Preliminary Recommendation 7:

[The working group recommends that ICANN org establish minimum requirements for the composition of the TAC (for example, minimum length, syntax, or entropy value) based on current applicable technical security standards. ICANN org MAY change these requirements in response to new or updated standards, but any changes to the requirements MUST go in effect with sufficient notification and time for contracted parties to implement the necessary updates.] OR [The Working Group recommends that Registrars and Registry Operators follow best practices for the composition of the TAC (for example, minimum length, syntax, or entropy value) based on current applicable technical security standards such as RFC9154 or subsequent or similar RFCs. These best practices may be updated in response to new or updated standards as appropriate.]

Sarah Wyld suggestion:

The Working Group recommends that Registrars and Registry Operators follow best practices for the composition of the TAC (for example, minimum length, syntax, or entropy value) based on current applicable technical security standards such as RFC9154 or subsequent or similar RFCs. These best practices may be updated in response to new or updated standards as appropriate.

Jim Galvin suggestion:

The working group recommends that the minimum requirements for the composition of a TAC MUST be as specified in RFC 9154 (and its update and replacement RFCs). In addition, where random values are required by RFC 9154, such values MUST be created according to BCP 106. [Footnote: BCP 106 is a Best Current Practice and is an idempotent reference to the most recent version of the specification entitled “Randomness Requirements for Security”, currently RFC 4086, which is how it is referenced in RFC 9154.] The salient specification point from RFC 9154 is as follows.

- Using the set of all printable ASCII printable characters except space and a required entropy of 128 bits, the length of the TAC MUST be at least 20 characters.

Gould, J. and R. Wilhelm, "Extensible Provisioning Protocol (EPP) Secure Authorization Information for Transfer", RFC 9154, DOI 10.17487/RFC9154, December 2021, <https://www.rfc-editor.org/info/rfc9154>.

Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005, <https://www.rfc-editor.org/info/bcp106>.

Preliminary Recommendation 9:

The working group recommends that:

9.1 The TAC MUST be only generated by the Registrar of Record upon request by the RNH or their designated representative.

9.2: When the Registrar of Record sets the TAC at the Registry, the Registry MUST securely store the TAC using a one-way hash that protects the TAC from disclosure.

9.3: When the Registrar of Record provides the TAC to the RNH or their designated representative, the Registrar of Record MUST also provide information about when the TAC will expire.

Jim Galvin suggestion:

9.2 When the Registrar of Record sets the TAC at the Registry, the Registry MUST store the TAC securely, at least according to the minimum requirement set forth in RFC 9154: using a strong one-way cryptographic hash with at least a 256-bit hash function, such as SHA-256 [FIPS-180-4], and with a per-authorization information random salt with at least 128 bits.

[FIPS-180-4]
National Institute of Standards and Technology, U.S.
Department of Commerce, "Secure Hash Standard, NIST
Federal Information Processing Standards (FIPS)
Publication 180-4", DOI 10.6028/NIST.FIPS.180-4, August
2015, <https://csrc.nist.gov/publications/detail/fips/180/4/final>.

Preliminary Recommendation 11:

The working group recommends that the TAC MUST be “one-time use.” In other words, it MUST be used no more than once per domain name. The Registry Operator MUST clear the TAC as part of completing the successful transfer request.

Jim Galvin suggestion:

The working group recommends that the TAC MUST be “one-time use.” In other words, it MUST be used no more than once per domain name. The Registrar of Record MUST meet this requirement by randomly creating a new TAC each time one is needed as specified in Preliminary Recommendation 7. The Registry Operator MUST clear the TAC as part of completing the successful transfer request.