Hi all,

I'm really uncomfortable with the idea of **adding** meanings to the AuthInfo field. As Paul Diaz notes in his comment to the list, the ICANN site offers the following definition of what the AuthInfo code is used for;

> "The AuthInfo Code is a unique code generated on a per-domain basis and is used for authorization or confirmation of a ***transfer request***. Some registrars offer facilities for you to generate and manage your own AuthInfo code. In other cases, you will need to contact the registrar directly to obtain it. The registrar must provide you with the AuthInfo code within 5 calendar days of your request."

So when people propose to also use the AuthInfo code to authorize a **different** action (whether it's change of control, or some other domain-name transaction), it raises flags for me. Here's a little outline as to why.

Question to registrars and registries -- would they like to do this process with the same credentials or separate ones from the existing AuthInfo (combined) model

The Issue for me has two parts – meaning and timing

Using the same long-lived data (AuthInfo) for different kinds of credentials creates operational and security issues

- Multiple meanings
  - Wikipedia -- "In practice, data elements (fields, columns, attributes, etc.) are sometimes "over loaded", meaning a given data element will have multiple potential meanings. While a known bad practice, over loading is nevertheless a very real factor or barrier to understanding what a system is doing." [sic]
  - During discussion I've been led to believe that AuthInfo codes are already being "overloaded" by organizations that use them as credentials for functions other than registrar transfer (eg WHOIS change, extending domain registrations, etc.)
- Varying lengths of time
  - Registry and registrar practices vary as to when the AuthInfo is initially set, when it is reset, what conditions require a reset and so forth. Thus some AuthInfo codes may be valid and available for years while in other cases they change over quite a short period of time. In addition to being confusing, this variability can also lead to security issues.

Examples of possible meanings of AuthInfo in production systems

- This person is authorized to transfer a domain name between registrars (this is the "official" meaning of AuthInfo code – the rest of the ones on this list are, presumably, "unofficial" uses of a convenient credential)

- This person is authorized to transfer control of a domain to a new entity
- This person is authorized to update WHOIS data about a domain name
- This person is authorized to perform a registrar-specific function, such as extend the registration period for a domain

Examples of the problems that these multiple meanings might contribute to

- a person with low security authorization (eg a tech contact authorized to update WHOIS data) could use the code to maliciously perform a higher-security function (eg transfer control of the domain)
- a similar situation could arise in a dispute between the Administrative Contact and the Registrant where the Administrative Contact uses the AuthInfo to perform transfer of control that they're not authorized to.
- a former employee could use a long-living AuthInfo to transfer control of a domain long after they've left their employer
- simultaneous transactions could overlap -- using the same data element raises the questions "which activity 'trumps'?" and "are BOTH of these transactions valid?"

Options to consider

- continue current practice -- add one more "overloading" to an already overloaded data element, allow registries and registrars to set their own practices with regard to creation, use and expiration
- use a new/different data element to authorize change of control transactions, leaving current (overlapping/ambiguous) uses and expiry practices relating to AuthInfo unchanged.
- use a new/different data element to authorize change of control <u>and</u> restrict AuthInfo only to the use for which it is intended
- change creation and expiry requirements AuthInfo to be very short -- setting the AuthInfo at the beginning of a transaction and expiring it immediately after the transaction is closed -- allow no simultaneous transactions using AuthInfo (eg simultaneous WHOIS update and change of control)

My preference leans toward the third one on this list – a new field, with a new name and a new meaning and restricting AuthInfo to its original meaning.

Dimensions to consider when making the choice

- data integrity
- process integrity
- cost to registrants
- cost to registrars and registries

Summary

I think this issue lies close to the heart of the “change of control” discussion. The Change of Control policy issue ultimately flows from “overloading” the Inter Registrar Transfer process with ambiguous and differing Change of Control components. The reason we're working on this is to see whether we can come up with a way to clarify the distinction between those two things.

Coming up with a clear distinction in policy and then re-muddling it by smashing the implementation of those now-different things into a single data-element seems to me fraught with peril.