Comment by the ID4me Association to the "Draft Technical Model for Access to Non-Public Registration Data" released by ICANN's Technical Study Group

The ID4me Association is a non-profit consortium of players from the domain name industry, willing to develop and promote an open and public standard, free from royalties and based on OpenID Connect and on the DNS, to allow any interested entity to provide Internet users with federated identities that can be used globally for single sign-on. The Association was originally founded by Denic, 1&1 Ionos and Open-Xchange and has now 20 participants (see https://id4me.org/).

We would like to thank the TSG for its work and provide a few technical suggestions that build on the proposed technical model and that could help its implementation.

Reusing existing identities

It is not clearly defined in the model whether the identities that are going to be used for authorization and authentication in the Unified Access Model are meant to be specific, i.e. solely released and used for that purpose, or are meant to be potentially usable in other contexts as well, and maybe release by any existing generic identity provider that makes itself technically compatible with the system.

We note that there is a general industry trend towards generic, reusable identities, as requiring each Internet user to maintain dozens or hundreds of separate accounts and identities is insecure and burdensome. The objective of distributed protocols like OpenID Connect is to support the use of one identity for any number of relying parties, allowing the user to own and secure a single set of credentials. We would thus recommend that ICANN adopts a system that is at least compatible with identities that can be used more broadly, though of course nothing prevents users that really want to have a UAM-specific identity to create a specific one just for that.

Supporting multiple identity providers

Actor models 2 and 3, as described in the document, require support for any number of identity providers. This would even be more important if ICANN wanted to support generic identities rather than UAM-specific ones. We also note that having multiple identity providers would possibly make the system much easier for the users, as they could reuse the identity from a provider where they already have an account, once it became interoperable with ICANN's system, or, if they needed a new identity, they could pick a provider near to them, in their language and country.

To support any number of identity providers within a single OpenID Connect deployment, unless all the relying parties have a pre-shared list of all existing identity providers that has to be kept up to date and that requires each user to pick the correct one every time before authentication, a "discovery mechanism" is necessary: a protocol that allows the relying party, given the identifier ("username") of the user, to determine automatically which identity provider is managing that specific identity, so to start the OpenID Connect authentication flow towards the appropriate server.

This was the problem that led to the creation of the ID4me effort, and that has been solved by specifying an extension to OpenID Connect that allows the discovery through the use of a DNS record. The extension has been specified in this independent Internet draft:

https://www.ietf.org/archive/id/draft-sanz-openid-dns-discovery-01.txt

as part of a broader architecture that is described in this other draft:

https://www.ietf.org/archive/id/draft-bertola-dns-openid-pidi-architecture-01.txt

Further standardization work at the IETF (or at the OpenID Foundation) has been deferred until the mechanisms are implemented and tried in practice, but we are glad to announce that the first product based on these specifications, Denic ID, is going to be launched in a matter of weeks, and the technology can thus be considered mature for use in other systems as well.

We think that ICANN should take the lead also from the technical standpoint and support the adoption of open innovative technologies, especially if, as the above ones, they are also meant to promote new uses of the Domain Name System and keep it relevant and useful in the long term, to the advantage of all ICANN stakeholders.

We would be happy to explain more in detail the workings and motivations of the ID4me standards to the TSG, and we suggest that they can be used to support any number of identity providers in the new RDAP access system.

Adopting the verifiable claims standard

Another new standard is just being introduced for online identity: W3C's Verifiable Credentials. It allow any third party to release and sign claims that can be incorporated within an identity and shown by the user to other parties, that can in turn validate the claims and thus trust them.

We think that ICANN should also adopt and support this innovative technology to deal with the transmission of vetting information from the authorizers to ICANN's gateway – or, if a decentralized model were later adopted, to the RDAP operators.

ICANN should then recognize the authorizers and assert their ability to release claims on specific qualities of the user that, coherently with any policy that will be agreed, determine his/her permission to access certain non-private data through RDAP; qualities like "is a law enforcement agent for country X" or "is an intellectual property lawyer practicing in Y". The authorizers would release these claims in the verifiable format, and the gateway, or any other interested party, could then validate the cryptographic signatures and be reassured on the validity of the claim, and of the authorizer itself.

Conclusion

Having worked to establish and promote DNS-based open, public and federated identities for the last three years, we would be happy to engage with the TSG and support the further specification

and implementation of the new access system for non-public RDAP information. We look forward to a reply and to such engagement; we thank you for your attention.

For the ID4me Association
Vittorio Bertola
Chair of the Governance WG