Yesterday you heard me push back on our current intention to keep using name and logo of inviter when we establish a connection. I am *really* concerned about the phishing potential. This feels to me like way more of a problem than the key management subtleties that have caused us such dissonance elsewhere. It is just asking for abuse -- and it's abuse that will subvert the entire DID-based ecosystem, because you'll start out with a false assumption about who you're talking to; everything downstream will be useless.

However, I do get that others in the space are showing name and icon, and we need the same UX. Plus, I get the need to be scrappy and fast.

The theoretical "right" answer is to decouple the C.M UX from the steps of a single protocol. Automatically accept all incoming connection requests, then challenge the remote party to prove their true name and logo with a VC, after the underlying connection has been built. Once the remote party has proved who they are, THEN ask the user whether they want the connection, showing a name and logo that's been verified.

But this theoretical answer doesn't help us. Even if we built it (which would take some effort we don't want to expend), today there are no issuers of VCs for orgs, so there's no way for an org to prove their name and logo. That might change with GLEIF, eventually. But not soon.

So I've been thinking, and here's an alternate idea that is moderately cheap, useful for the foreseeable future (doesn't have to be deprecated), acceptably secure, and capable of supporting the UX we want. It also gives us some nice talking points about interop, as a side benefit. Plus it solves a bootstrapping problem in a way that will grow the ecosystem.

1. Add to an invitation a field called "domain" that contains a host name like "www.acme.com". Also add a field called "avatar". Domain would be used by orgs or by people who own a personal internet domain; "avatar" would be used by people who don't have a domain.

2. If "domain" has a value in an invitation, activate the following validation logic.

* Fetch /.well-known/did-configuration.json and validate it per https://identity.foundation/.well-known/resources/did-configuration. We expect the DID of the inviter to be the DID of the domain owner, and we can prove it by validating a self-issued VC published on their web site. (This will require us to implement very simple support for issuing and validating non-anoncreds VCs. I estimate this to be two person-weeks of effort. We will be able to claim some basic interop with Microsoft and Digital Bazaar as a result -- enough to tick boxes, but not enough to be gloriously robust.)
* If the well-known DID validates for the specified domain, then fetch the domain's favicon the same way a browser would. Display the name of the inviter from the VC, and the favicon from the domain, when we show the user the invitation. Put a nice green checkmark badge on top of the icon to show that we have verified the identity of the sender.

   * If the "domain" value doesn't validate because there is no /.well-known/did-configuration.json file, go to 3 below.
   * If the "domain" value doesn't validate, pop up a big red error telling the user that the inviter is claiming an identity but explicitly failing to prove it. Don't allow them to make the connection.

3. If no claim is being made about the "domain" of the inviter, then alert the user that the identity of the inviter is not validated, and warn them that this could be used to phish. Urge them to challenge the remote party for credentials as soon as possible.

I suspect others in the Aries space would be willing to support the same feature.

The one downside to this approach, other than the effort, is that any org that wants to invite people will now need to issue themselves a VC that's not in anoncreds format, and publish it on their website. This might be an annoyance. However, with the person-week of effort that we spend on issuance, I think we could produce a simple script or tool that would do that for them.