VA Lighthouse Governance Model Microconsulting

Moncef Belyamani

18F Login.gov team

7/5/2018

## Questions

* Tell me about your role and responsibilities

We don’t think of ourselves as API managers. SAML or OpenID connect. Most people are using OpenID Connect, only one agency on SAML.

Moncef Belyamani - login.gov, BE, be on since the beginning

Steve Ersioli (sp?) - login.gov, since dec, on agency integration team

* Role on project (Login.gov)?
* How are they staffing it? Running customer onboarding and service?

Have a sandbox so they can do self-service. Coworker (Vishal) are tier 1 for help desk. Tier 2 is Steve and other engineer.

We pitch to agencies to get them onboarded. Sometimes a mix of both, agencies coming to us and us going to them. We have a pitch deck we use to give them information (they will send us slideshow).

On board about 2-3 agencies per sprint.

Team is 18F or USDS, some contractors, AWS consultants. DevOps team, end user team focuses on secure.login.gov website (design, researcher). Agency research team (Steve and Vishal), Joel Mintan (sp?) pitches to agency, DevOps takes care of infrastructure.

Doing their own AWS instead of cloud.gov, since it wasn’t up when they started. Not sure if it could now support the 6 million users.

Maintain a database of 6 millions users’ information. That way agencies don’t need to manage authentication, worry about security, etc.

* Who is on the team that we should also talk to?
* Informational on what we’re doing
* How does building APIs in the gov work?

## Authorization frameworks

* Tell me about the thought process around 2fa
* What is the timeline for LOA3?

Login.gov LOA3 - working on it but it’s not launched. Expected timeline 1-2 months. Was originally going to use Equifax but now need to use a different provider.

We have separate vendors for verifying drivers license, address, phone number, etc.

Railroad Retirement Bureau is the only one we currently know of using LOA3, for some kind of benefits program.

A lot of times agencies believe they are LOA3, but reality is their are LOA1. How users present data is different than how they get access to the data.

* What governance/guidelines do you have for what data you share with whom?

OPM governance guidelines

Syncing email addresses from USAjobs. They determined that was the easiest path, so we made sure on our end that we would display a message on the screen that says “hey, make sure you use the same email address”, and make sure they display the same information on their website.

Not part of that team, but I think we helped them create that content and strategy.

Global Entry - didn’t go so well because they didn’t head our advice, they only tested with five internal users. We still get emails sent to login.gov because the CBP’s website makes it hard to contact them, so people email us about their global entry accounts. We sent them emails they could send to users but they didn’t use them.

So if an agency wants to integrate with us they need to have best practices, good documentation, and plan with us in advance, documenting questions people could be asking.

2FA - mandated by login.gov. We offer more options now, before it was only SMS or voice to get the security code. Now once you create this account you can create an authenticator app, but you only see that if you continue on the login.gov page. Most of the time after you create the account you get sent back to the account page. So that was confusing.

So now during account creation we have a 2FA setup page, you can choose between PIV/CAC, sms, authenticator app. We’re talking about doing multiple options at once as well.

* What source of data standards did you use in building out the API? How did you write those policies?

OPM, only share users’ email address.

Each agency can request what attributes they want to receive. But, if an agency wants to use SSN, but they only have a LOA1, we won’t allow that.

Attributes: email, phone for LOA1 users.

If you request an account deletion, we won’t do it right away, we send an email, wait 24 hr, etc, in the instance it’s a malicious users.

LOA3- first name, last name, address, SSN, driver's license

We maintain that information in our database encrypted.

## Closing Questions

* Is there anyone else that you think would be good for us to talk to?

Sam.gov, allows you to do business with the government, contracts. Rolled out this past friday.

Registry of certified medical professionals

Move.mil, for service people moving

Ngageoworks.portal, weather information

From your team:

Andrew Huey (sp?) UX