UX Analysis

## Table of Contents

[API Consumers Experiences](#_svzr3lm4v4hw) 1

[End-User Experience Do’s](#_l4y1suf43tom) 4

[API Provider/Owner Do’s](#_6fm8tmfad5am) 5

## 

### API Consumers Experiences

* Motivation for using API = not having to store usernames and passwords and gaining 2FA (security reasons), better performance (scalability of AWS), help in managing user access/account help

*“I think the goal of integration was that we didn't want to have to manage the NIST guidelines. So it was more of, we don't want to be in the business of logging people anymore from a performance perspective. We do gain some availability there because they are in AWS, the cloud, and we are not. So, you know, our scalability is going to be a much slower than logins’ would...Before we had login.gov, we managed everything internally.”*

*“So login.gov gave us two factor authentication, which allows us to reduce the friction.”*

* Benefits of using API = reduced cost of storing data, no longer need to store passwords/usernames, improved security/simplified security requirements, always up to date on security guidelines, frees up team to focus on purpose of usajobs

*“Yeah. Um, I think a lot of the benefits are more that we don't have to worry about any kind of NIST guideline changes that happened. Before, you know, if this came out with a new guideline, like you have to do this or that we would have to make adjustments. Now if they’re adjustments made to NIST, it's more on login.gov to make that change. I guess another benefit would be we don't store passwords anymore, right? So I don't have to know a user's password, which means no one can kind of hack us through our own database anymore.”*

*“..[login.gov] does, it takes that burden of authentication off of us. Everything from NIST guidelines to security issues, to even a reduction in security issues, and even.. help desk traffic tickets…”*

*“Authentication, it's just something that has to happen to be there, but it's not like the main function of our site. The main functions of our site is to help folks find and apply to jobs and that's a much bigger authentication was just kind of the in their way. And so now hopefully we can focus on the things that are more core to our quote unquote business.”*

*“They can provide the best possible user experience for authentication and we can focus on everything that happens after that.”*

* Previous method of identity-proofing = email and security questions

*“So the only thing we use to identify users to basically prove that they are who they are is through email... And we all had security questions too.”*

* Future benefit of api = streamlining hire by automatically sharing important documentation

*“So, you know, there was some discussion I think amongst the top brass about whether we should try to push for LOA3 and have that. There was some interest in that I think mainly because, you know, agencies also have a desire to streamline folks through their onboarding process once they do make a hire. So it would save potentially save them some work if, if you knew exactly who was somebody was, you could tie that to their SF50 or D214 or whatever it might be.”*

* 2FA and end user challenges, user complaints centered around 2FA requirements

*“[user complaints centered around] inconvenience of two factor essentially, which was not really going to be any different if we had done it versus login.gov doing it.”*

* Solution: “Remember computer feature” helped relieve 2FA ux issues
* Integration issues = connecting user names and emails, switching to email as primary identifier

*“One [issue we experienced when integrating] was we had previously accepted a username as well as a primary or secondary email. So some folks who were using their username didn't remember what email they had their account attached to there were certainly in the minority but a healthy number nonetheless. And so when we transitioned in and we asked folks to use their primary, secondary email, because that would be the way that we would automatically connect their login.gov account to their USAjobs profile. If they were using that username and couldn't remember the email, they were kind of a little bit out of luck. They'd have to contact the help desk and provide their username and their security answers, which, you know, they can't remember their email. They're very unlikely to remember the answers to their security questions either.”*

* Implementation experience. Only problems were with configuration, unexpected releases

*“I think the team was very helpful, you know, the, the login.gov team was helpful when we needed them…. I guess they have very good documentation because we didn't have to reach out to them too much.”*

*“One of the big hurdles we had after, after we did the integration, users have authenticated with USAjobs through login.gov. they've established this linking between the two sets of accounts and after that Login.gov released the capability for users to delete their login.gov accounts. It was kind of an unanticipated thing. We didn't know it was coming and when it released we discovered that users now have the ability to orphan their USAjobs account, delete the login account.”*

* Configuration challenges, lack of visibility re configuration before dashboard was problematic

*“If we did have any questions, it was more on the configuration side, you know, they actually have configuration about who can call them. So we had to configure our site as a valid caller to login.gov...At the time it required a lot of intervention with login.gov,... emails back and forth...They have since done a whole new dashboard where you can kind of go in and see what configurations you have out there and you can actually add the configurations yourself instead of going through them. So that helped out a lot.”*

* Solution: Login.gov created a self-service dashboard for configuration which helped a lot.

### End-User Experience Do’s

* Redirect user to where they need to go to be successful (eg after creating login.gov account)

*“So once the login is completed, where does the user get redirected to? I have to put that in the configuration as well.”*

Example images:

Login.gov → Global Entry

* After integration, provide guidance to users on how to navigate/manage the new system

*“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.”*

Example images:

Login.gov

* Provide multiple 2FA options (app, phone sms, phone voice, authentication link from email etc), and explain when necessary why these security features are in place

*“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.”*

*“If anything I would rather move away from passwords totally. And have it be a link that they authenticate with because they do only use it once.”*

Example images:

Login.gov

Walgreens

* Use plain language in privacy policies and terms of service

Example images:

Google

* Allow a user to easily see who has access to their information

Example images:

Google

Facebook

* Allow a user to easily revoke a third parties access to their information

Example images:

Google

Facebook

Blue Button

* Make it obvious what data is being shared when authorizing third party applications

Example images:

Google

Blue Button

Login.gov

* Allow a user to access all their data associated with an account

Example images:

Google

Blue Button

### API Provider/Owner Do’s

* Use past experiences of end user results to inform decisions when implementing with new consumer

*“I would say they were able to provide us guidance based on previous projects. They had just gone through [integration with] Global Entry and working with them so they were able to tell us, you know, kind of use that as a use case and say, well, in that case we would advise because of our experience, they're not to do this and maybe try this other thing.”*

* Provide self-service options to developers as much as possible

*“They have since done a whole new dashboard where you can kind of go in and see what configurations you have out there and you can actually add the configurations yourself instead of going through them. So that helped out a lot.”*

*“That dashboard and the integration environment work perfectly.”*

* Provide open lines of communication about releases to API customers

*“If we had known a delete account feature was coming up a relatively soon, you know, maybe a couple months out, then we could have had a lot of discussions on that and see what changes we want to make on our side to meet that new feature that being implemented...I think having a roadmap would be nice...These are things we’ll be working on the next couple of months. And based on those... we can go ahead and address anything that we need to fix on our side.”*

*“I think because of that change [releasing a new feature] we asked for more advanced notice of what changes they're making because we were sort of getting them like the morning of.”*

* Provide versioning of APIs
  + Versioning standards are best practice for easier integration and future development

[pace of releases in gov is slow, agencies need time to adapt/budget for changing to new versions/updating their systems as needed]

*“..typically an API would follow a versioning best practice where there would be a version endpoint that was stable so that all the groups using that API could develop against it and you know, sort of have their flexibility to do what they needed to do. But then also giving the team who's developing that API, the ability to develop the next version independently of all of the groups using the API.”*

* Embed provider team members if possible during integration phase

*“I'm just back to your earlier question about, you know, what did login.gov provide us and maybe what, what would have been better or what maybe what did work. They did provide the design team, a designer to work with who had worked for awhile on their, on their interface, they could answer questions about the decision, the design decisions they made there, um, as well as help vet our designs for possible problems. He was just a really great reference for my team and myself… to bounce ideas off of and to ask questions… He was a guest in our slack and vice versa….So we were able to get fairly immediate answers when we are in the design phase.”*

* Give consumers data on use case experiences that help sell reluctant state holders on value of integrating

*“We've mostly tried to answer from our perspective: this is the benefits and this is what it's costing us today and what have you. But they [login.gov team] actually did help quite a bit with convincing folks this [integrating with their API] is the right way to go.”*

* Provide comprehensive documentation

*“I think bad documentation would be documentation that excludes steps….Bad documentation would be, I make the first call, it gives me a peace to authentication, but they don't list what I need to do next to get the next piece of authentication...As long as all the steps are there and defined and I know exactly what I need to call, what information I need to pass, I think the documentation is good.”*

* Have good documentation, it will help drive adoption

*“Same thing with documentation, you know, that's not only impacting development time, but that's also impacting adoption where, if I learned about a new API but there's no documentation or incomplete documentation or I can't easily try out requests see responses. You know, that's going to limit the amount of interest someone might have and in actually adopting and using that API.”*

* Reinforce best practices amongst consumers

*“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.”*

* Protect end user privacy and maintain high security standards

*“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. LOA3 attributes are first name, last name, address, SSN, driver's license. We maintain that information in our database encrypted...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.”*

*“I think we would want to keep some review process, it’s hard for me to imagine in the medium term anyone getting comfortable with letting people straight into prod without a check on it. We have a demo meeting with the customer, they walk us through the application, and then we ask them questions about privacy policy/terms of service, how they handle security and data breaches. “*