National Institute of Standards and Technology

NIST Website About NIST usnistgov on Github

Digital Authentication Guideline: Public Preview

- **SP 800-63-3**
- **SP 800-63A**
- **SP 800-63B**

- **SP 800-63C**

Welcome to the NIST SP 800-63-3 Public Preview! We're excited to share the major transformation that this document has undergone, as well as collaboratively enhance and evolve the guidance as we head to a public draft later this summer.

A few formalities

Public preview vs public draft

If you've made it to this page, you can see we're approaching this a little differently by putting our work up on GitHub, rather than the "traditional" comment period for a NIST Special Publication (SP). We're calling it a public preview because some of our agency partners (and NIST itself) have formal processes for public drafts. Calling it a public preview is our way of letting everyone know those processes aren't in play. This lets us do things differently…

A different cadence

This public preview is focused on gaining input through successive open comment periods and editing iterations of the SP draft. This phase will include multiple iterations of comments of approximately 2 weeks in length, followed by a 2-3 week period for the editors to adjudicate comments and make appropriate updates to the document.

We'll continue iterations for as long as we have feedback that results in meaningful changes. We welcome you to come back every iteration to see what's new, or watch daily. While we'll be posting major iterations every few weeks, we'll also make updates mid-cycle.

The first release

The work represented here is considered a stable draft, reflective of what NIST has learned about industry innovation, new threats, and an evolving landscape of federal digital services. We have heard and learned so much through public comment periods, Executive Order 13681 – Improving the Security of Consumer Financial Transactions, public workshops, and feedback from NIST's ongoing work such as NSTIC pilots and NCCoE industry collaborations.

But this release is neither complete nor perfect–and it's not intended to be. Rather, we believe we're at a point where we've articulated the direction we're going, but need our stakeholders to comment on what we got right, what we got wrong, and what we missed all together. We know that while SP 800-63 is scoped to federal agencies only, it has material impact on our

private sector partners. So we want to put fingers to keyboard with the community earlier and more often in hopes this update to SP 800-63 not only reflects the current state of the market, but has a level of future-proofing for where DIGITAL authentication to government services is going. (Apologies to those that loved the term e-Authentication, but it's 2016, folks!)

A quick summary

Here's a quick list for the biggest changes we've made, but you'll need to dig into the documents (yes, *documentS*) too:

1. LOA is decoupled into its component parts
2. Complete revamp of identity proofing
3. New password guidance
4. Removal of insecure authenticators (aka tokens)
5. Federation requirements and recommendations
6. Broader applicability of biometrics
7. Privacy requirements (under construction)
8. Usability considerations (under construction)
9. And many more…

Please note that the privacy and usability chapters are under construction. We wanted to establish a baseline set of requirements before we plunged into those sections. Expect to see content there in the future iterations, and we welcome suggestions!

Why GitHub

Ok, "Why GitHub?" you ask. For us, the choice was relatively straightforward. GitHub has been a mainstay of the development and standards communities for many years now, serving as a space for collaborative interaction, the epicenter for evolving open source software, and an essential component in every coder's toolkit. It only seemed appropriate for us to engage where so much of our community already congregates and collaborates.

Second, as a platform, GitHub has many unique characteristics that make it attractive as a place to develop this special publication. From its ability to support broad engagement, to excellent version control, and multiple avenues for collecting and receiving input—it is a robust forum suited to this phase of drafting the 800-63-3 suite.

Overall, GitHub is the right tool for the job. But this is a new process for us; we don't want to leave anyone out, and we anticipate some growing pains as we work this out together.

To that end, our use of GitHub is additive to the existing open and transparent process that NIST already follows. If you don't have the time this spring and summer to keep up with us, don't worry. We will maintain our tradition of extended public comment after this process comes to a close.

However, to manage this phase properly, we sincerely request that commenters provide substantive input. Editorial or general comments will be accepted begrudgingly. We want substantive technical/procedural comments. We'll get to the grammar and formatting later. Trust us, this is as hard for some of the rather strict grammarians here at NIST as it is for anyone!

In addition, commenters are **STRONGLY** encouraged to collaborate with the team and other public participants via GitHub issues. See this page for details on how to submit a comment to us. We want to maintain a lean approach, so we are discouraging email and Excel files during this phase. We thank you in advance for your efforts to keep this process streamlined for the editors.

So have at it! We're really excited about the changes we've made - we think you will be too!

Source information, current standards, and public comments received through May 2015 can be found here.

- **SP 800-63-3**

- **SP 800-63A**

- **SP 800-63B**

- **SP 800-63C**

Privacy Policy | Security Notice | Accessibility Statement | Send feedback Get help with leaving a comment