Government Adopts an Industry Approach to Open Source Collaboration

Paul Grassi, Mike Garcia, and Katie Boeckl, NIST

In response to recent increases in massive identity-centric security breaches, NIST has released a significant update to Special Publication 800-63, Digital Identity Guidelines, *which lays out technical and procedural requirements for US federal agencies that need to authenticate users accessing their digital services. This update took a new approach—open source document development—to more intimately involve stakeholders in the revision effort.*

NIST's guidelines like *Special Publication (SP) 800-63, Digital Identity Guidelines* (www.nist.gov/itl/tig/special-publication-800-63-3), are often mistaken for standards, although they are guidance that applies only to federal, non–national-security systems. Still, they're useful to a broader audience. Thus, we sought to serve our stakeholders both within government—after all, this guidance is for government systems and services—and the private sector, which creates the technologies these systems rely on.

We needed a thorough yet speedy update, and the best way to achieve both called for the combined efforts and expertise of all stakeholders: NIST, the private sector, and our government peers. The closer the collaboration with all parties, the more likely the final guidelines would be effective, implementable, reflective of technologies in the market, and flexible enough to neither stifle innovation nor box it out of future federal use cases. And because the digital identity community stretches across the globe, we also needed our international stakeholders. We wanted the community to be collectively proud of, and approve of, the final product.

0018-9162/17/$33.00 © 2017 IEEE

EDITOR **CHUCK WALRAD**
Davenport Consulting; cwalrad@daven.org

TAKING A NEW APPROACH

A few changes were in order. We needed to find a way to give stakeholders the pen to contribute text directly to the document, while also respecting the processes many government officials use to effectively collate their agency's feedback. The federal government can be a bit cautious, so we knew not all agencies would be able to participate in this new, very public manner, especially without vetting by their digital identity leaders. We also didn't want to integrate feedback into the guidelines in a silo within NIST. Because we couldn't have every stakeholder sitting at an actual table, we wanted a way to do so virtually, allowing any interested party to discuss comments, and to build consensus around the best way to reflect these comments in the document.

GitHub—an online development platform for hosting, managing, and building projects collaboratively—fit the bill. We hosted the draft publication on GitHub and asked stakeholders to dig in and comment on what we got right, what we got wrong, and what we missed altogether. We wanted to make sure the *SP 800-63* update reflected the current state of the market and achieved a level of future-proofing to accommodate innovation in digital identity.

Organizations like the Fast Identity Online Alliance, the Internet Engineering Task Force, and the World Wide Web Consortium host documents in public GitHub repositories. Even the White House Office of Management and Budget did the same with Circular A-130, Managing Information as a Strategic Resource. But this type of process had never been leveraged by NIST.

TO GITHUB

Procedurally, it wasn't all that hard or different from what NIST normally does. What changed most drastically was the number of touchpoints with stakeholders. Our communication with stakeholders, as well as their communication with one another, was dynamic. With near immediacy, stakeholders could see and respond to changes we had made to the draft in response to their input. GitHub gave us the power to get feedback—positive and negative—as quickly as stakeholders could type it (see Figure 1).

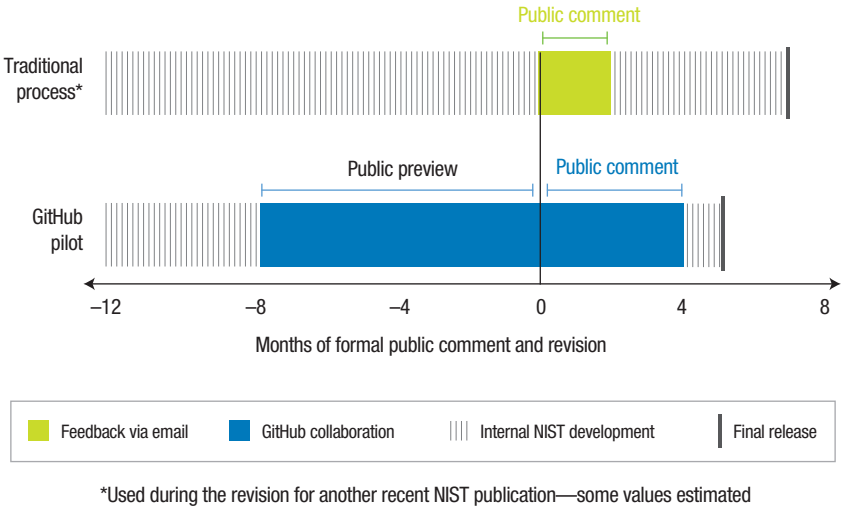

Figure 1. Process comparison showing the increased collaboration time we could offer on GitHub.

In general, it's better to throw something out there that people can comment on than to give them a blank sheet of paper. So we started internally by building a draft. Once we had what we considered a "stable draft"—complete enough to demonstrate what we believed we had heard from the community—we put it on GitHub. We launched this "public preview" of *SP 800-63* in May 2016. We ran four iterations, each a month long, in which we received comments ("issues" in GitHub speak) and edited the document in near real time in response. In hindsight, the iterations blurred together to the point that managing distinct iterations was pointless. But we ultimately got what we wanted out of it: four months of consistent contact, feedback, input, and debate on what the document needed. We even had community members directly contribute text via GitHub "pull requests," which alert authors when someone submitted content for consideration. If we liked it, we approved and merged the content into the document. If we didn't, we commented back to the submitter, collaborated on changes, gave them time to make the edits and resubmit, and then merged the updated content into the master document.

At the end of September 2016, we asked our stakeholders for a period of calm and closed the public preview period. However, the document remained public, and we triaged any issues that came in as we got the document ready for its formal "public comment" period. The holidays impacted our timeline—no one wants to read and comment on pages of

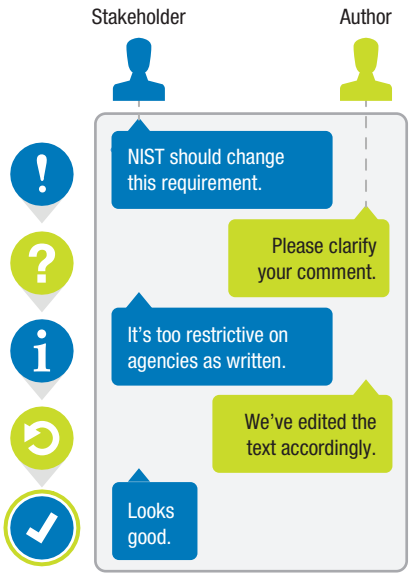

Figure 2. A hypothetical scenario showing collaboration between an author and stakeholder in the piloted process.

technical requirements between late November and early January. When the new year began, we resumed by launching the formal comment period, which ended up being 90 days of collaboration.

We really wanted people to use the online document, but to respect the traditional process (and those who weren't comfortable with GitHub), we made a few adjustments and ran some workflows in parallel during public comment:

- In addition to the online document, we offered stakeholders a PDF.
- We knew not all agencies would or could provide comments via GitHub, so we provided a comment matrix spreadsheet for submitting comments via email.

This is where it gets interesting. Traditionally, when NIST receives comments via email, we share them online at the same time the document goes final. In this case, we wrote a script to automatically take the comments submitted in a spreadsheet and upload them to GitHub as issues, attributing them to the original submitter. We wanted one source for all feedback, and GitHub—not our inbox—was that designated place.

One point on which we must commend even those who didn't use GitHub: No matter how we requested them, we often got "comments" in the form of lengthy letters, with paragraph prose. These letters are incredibly difficult to work with to make actual changes in the document. When we received such a submission, we asked the commenter to go back and put their feedback into the spreadsheet so we could use our script to upload to GitHub. Every single commenter took the time to do this. They saw the effort we were putting into this more open approach and responded in kind.

We kept the online version stable—meaning no changes were reflected in the master document. This meant an agency that downloaded it on day 89 saw the same version as someone that downloaded it on day 1. However, we maintained another branch in GitHub that reflected our continual edits without impacting the master document. The nice thing about this was that stakeholders could watch the editorial process and still contribute directly to the document. By allowing stakeholders to see how we interpreted their words, they could immediately notify us if we read them wrong.

By all counts, the new process worked. Collaborators submitted more than 1,400 comments, we approved and merged almost every external content submission, and the web version of the draft publication drew over 74,000 unique visitors.

SUMMARY OF BENEFITS

From the draft version to the finalized publication, we witnessed a few key benefits.

First was communication. Throughout the revision process, the community had a direct line of communication with us and with other stakeholders (see Figure 2). Each issue, due to the GitHub platform, essentially became a discussion forum. Stakeholders could agree or disagree with one another, and then come to a reasonable conclusion with a concrete suggestion for how we could improve the guidelines. If someone submitted a comment that seemed confusing, we could respond and ask for more details, clarification, or information sources. This level of engagement can't occur when using the traditional model of guidance (or standards) development.

Next was editorial power: stakeholders could make direct edits to the content by sending suggested changes to us through their own pull request. When we made edits based on an issue, we could "mention" (similar to a Twitter mention) a commenter in the update and ask if the change appropriately addressed their concerns.

Finally, there was enhanced visibility. Stakeholders could watch the guidelines evolve. GitHub's "compare view" breaks down publication changes line by line, including deletions and additions. Stakeholders could sign up to receive notifications when we addressed their comments. We labeled issues with tags like "accepted," "partially accepted," or "declined" to inform commenters exactly how their feedback would impact the document.

LESSONS LEARNED

The publication will remain on GitHub in preparation for future revisions using the same process. We plan to streamline internal review cycles to drastically shorten—or even do away with—the public preview phase.

In addition, the name "public preview" was misleading; some stakeholders skipped this phase and waited until "public comment" to share feedback. We understand that many could not commit as much time to this effort as we did and will adjust accordingly next time.

During public preview, we were changing so much so quickly that we ended up frustrating stakeholders who

wanted to read the document offline—by the time they came back, too much had changed. So, if we hold public preview phases for future publications, we will maintain a stable, unchanging version of the document, as we did in public comment.

Agency outreach is key. Agencies often managed comment creation internally, then submitted to NIST via spreadsheet because it appeared more controlled. But one agency proved that this level of management can also be achieved with GitHub. It collected comments internally, consolidated them into a unified submission, and then entered each comment into GitHub. Although this was outstanding, we will keep the automated script for uploading issues in a spreadsheet to accommodate all stakeholders.

We plan to release sets of implementation guidelines for *SP 800-63* to improve digital identity services. We have already published a set of frequently asked questions to address any recurring inquiries from the community and are open to additional questions.

We are ecstatic with how the process helped the community engage and with the quality of the resultant digital identity guidelines. We will strive to find ways to involve stakeholders even more in our process in the future. On the whole, we believe—and the feedback we received corroborates—that this process was a hit. We will continue to use and evolve this method of developing documents that mean so much to such an important and large community.

MIKE GARCIA is the Trusted Identities Group lead at NIST. Contact him at michael.garcia@nist.gov.

PAUL GRASSI is the senior standards and technology advisor at NIST. Contact him at paul.grassi@nist.gov.

KAITLIN BOECKL is a privacy risk strategist at NIST. Contact her at kaitlin.boeckl@nist.gov.