BETTER IDENTITY COALITION

Comments to NIST

SP 800-63-4 Digital Identity Guidelines (Second Draft)

October 2024

The Better Identity Coalition appreciates the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on its second draft of its fourth revision to the four-volume suite of Special Publication 800-63, Digital Identity Guidelines.

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 22 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, fintech, payments, and security.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at https://www.betteridentity.org/.

In July of 2018, we published *Better Identity in America: A Blueprint for Policymakers*[1] – a document that outlined a comprehensive action plan for the U.S. government to take to improve the state of digital identity in the U.S. Privacy is a significant focus: the Blueprint detailed new policies and initiatives that can help both government and industry deliver next-generation identity solutions that are not only more secure, but also better for privacy and customer experiences.

We note that we are encouraged to see NIST launching this new revision of SP 800-63-3. While the 2017 publication of SP 800-63-3 represented a significant improvement in NIST's Digital Identity Guidelines, technology and threat are never static. We believe there are a number of places where industry and government alike will benefit from a refresh of Guidance that reflects changes over the last few years. We are encouraged that NIST is embarking on another revision of the document, and that NIST took the time to release a second public draft given all of the feedback received on the first draft and the significant changes made in this latest version.

In January 2023 we submitted extensive comments to NIST on the first public draft of SP 800-63-4. Our comments here will be much more brief – in large part because many of the points that we raised have been addressed in the new draft. Note that we are not submitting any specific comments in the Excel template for line-by-line inputs; our comments here are more general in nature.

1) The addition of language representing mobile driver's licenses (mDLs) and verifiable credentials (VCs) is a welcome addition to the suite of documents. As industry and government work together to close the gap between government-issued physical credentials and the lack of robust digital counterparts – an area where NIST is leading critical work through the NCCoE mDL project – it will also be important to create guidance on where new digital counterparts to physical documents like mDLs can be used in ID proofing, as well as how relying parties (RPs), identity providers (IDPs) and credential service providers (CSPs)

[1] See https://www.betteridentity.org/s/Better_Identity_Coalition-Blueprint-July-2018.pdf

should look to implement and support them. NIST is to be praised for its forward-thinking approach here to build in support for these new types of credentials into these guidelines. We do note that as VCs and mDLs further mature in the marketplace, NIST may need to create supplemental guidance at some point to account for just how VCs and mDLs may be used, and/or update this next revision with additional language. However, the fact that this draft references them demonstrates that NIST recognizes their utility and also helps to "future proof" this document.

2) We also appreciate the work NIST has done to create guidance on the use of syncable authenticators. Synced passkeys are a new authentication tool that is transforming the authentication landscape and creating a valuable new option for implementers to improve both security and usability. However, as with many new security technologies, there is often a gap between their emergence in the marketplace and industry and government willingness to adopt or recognize them; this is particularly a challenge in regulated industries. Similar to the above comment on mDLs and VCs, we commend NIST for their forward-thinking approach to recognize this new technology and outline where and how it can be used in the broader authentication ecosystem.

3) Among the questions that NIST asked in the introduction to the new draft was: *"What specific implementation guidance, reference architectures, metrics, or other supporting resources could enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines?"*

   Here we think additional work is needed – if not in SP 800-63-4, then perhaps in another NIST publication – to create a "playbook" of standards and best practices that agencies at all levels of government should follow when creating digital counterparts to physical credentials – as well as attribute validation services – is needed. Some of this may be delivered as part of publications that will emerge from the NCCoE mDL project, which many Better Identity Coalition members are participating in. However, we think beyond technical guidance, it will also be important to provide guidance on policies and best practices to follow for both issuers and RPs – for example:

   a. How mDL guidance can apply to other government issuers of digital credentials. We note that one major technology platform is already offering the ability to digitally store a US passport in that platform's wallet – but doing so without any formal involvement of the State Department. It would be helpful for NIST to look beyond the driver's license to more broadly encompass other digital credentials, such as an official digital counterpart to the passport, a digital SSN card, state-issued digital birth certificates, etc. Americans should be able to ask any agency that has already issued them a credential in the physical world to vouch for them in the online world, and it is essential that there are consistent standards and best practices for issuers – particularly given that some agencies who issue physical credentials may not have the knowledge or resources to properly manage the issuance and management of digital counterparts.

b. On the relying party side, more work is needed to outline best practices for what RPs should and should not do when consuming digital credentials. For example, how can RPs ensure that the data they are requesting for is proportional to the risk of the transaction – enabling a default practice of data minimization? Are there ways that wallet providers or credential providers might be able to create guardrails against inappropriate requests for digital credentials or data from them? We expect as digital credentials start to emerge for online use cases that more attention will need to be paid to these issues.

c. It will also be important for NIST to further define what it means by “user control” (as referenced in SP 800-63C-4.2). Some stakeholders have raised concerns that users will not be truly in control if a credential or wallet provider is able to limit or disable a user’s ability to use a digital credential; others have noted that there may be some limited circumstances where it would be appropriate, provided that proper processes were followed (i.e., in the event that information came to light suggesting a credential was fraudulent).

We greatly appreciate your willingness to consider our comments and suggestions, and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition’s coordinator, Jeremy Grant, at [redacted].