Digital Identity Guidelines (NIST-800-63) Comments

CCG Response to Digital Identity Guidelines (NIST-800-63) Request for Comments

Draft Community Group Report 12 August 2020

Latest editor's draft:

https://w3c-ccg.github.io/nist-dig-comments/

Editors:

Wayne Chang
Emily Fry
Nader Helmy
Ken Huang
Christopher Allen

Author:

Credentials Community Group (W3C)

Participate:

GitHub w3c-ccg/nist-dig-comments
File a bug
Commit history
Pull requests

Abstract

This document serves as a collection of the W3C Credentials Community Group responses to Digital Identity Guidelines (NIST-800-63) Request for Comments. Please note that this is *not* an official W3C position, but the compendium of feedback from the Credentials Community Group, which is a group consisting of W3C members, W3C working group participants, industry, and the general public.

Status of This Document

This specification was published by the Credentials Community Group. It is not a W3C Standard nor is it on the W3C Standards Track. Please note that under the W3C Community Contributor License Agreement (CLA) there is a limited opt-out and other conditions apply. Learn more about W3C Community and Business Groups.

Comments regarding this document are welcome. Please file issues directly on GitHub, or send them to public-credentials@w3.org (subscribe, archives).

If you wish to make comments regarding this document, please send them to public-credentials@w3.org (subscribe, archives).

Table of Contents

1. Introduction §

This collection of comments is by no means comprehensive, but represents select perspectives from the community that we hope NIST will consider in its Digital Identity Guidelines. Many of the comments are synthesized from the artifacts and comments in the following GitHub issue thread:

https://github.com/w3c-ccg/community/issues/145

Most of all, these comments are meant to begin dialog and discussion with respect to the NIST Digital Identity Guidelines. They are not meant to be a final and definitive community stance, but an opportunity to begin engagement with government technologists and state-sponsored standards developing organizations including NIST and its affiliates.

2. Comments by Topic in "Note to Reviewers" §

Privacy enhancements and considerations for identity proofing, authentication, and federation, including new developments in techniques to limit linkability and observability for federation.

- Decentralized Identifiers have authentication required as a core DID Action. This means that the authentication follows the identifier instead of necessarily being determined by the system, reducing the implementation effort overall if there are DID Methods are appropriate for the use case.
- Verifiable Credentials can be relied upon by verifiers for authentication, and this use case enables a model where a separate trusted party can perform authentication in an interoperable fashion. See the example in the next section with SMS.
- See the comments for Section 8.1.1 for a usage example with Social Security Numbers
- Recent advancements in the community using zero-knowledge proofs with Verifiable Credentials have enabled selective disclosure functionality, using the BBS+ and Linked Data formats. This has significant privacy preserving and observability implications, allowing credential holders to present only relevant aspects of their credentials in a cryptographically secure manner.

Continued use of short message service (SMS) and public switched telephone networks (PSTN) as restricted authentication channels for out-of-band authenticators.

- Verifiable Credentials can assist with interoperability of existing SMS and PSTN authentication channels by providing means to package attestations, such as, for example, that a user can receive SMS messages at a specific phone number, in a standardized web-friendly format that is cryptographically verifiable. This approach enables further modularity at two critical junctures:
    1. The issuers of these authentication data do not have to be the same parties as the service being accessed; the standards imply an interoperable way to package this so a single entity can securely perform authentication on behalf of many others.
    2. With a generic way to package reliable authentication information, we can prepare existing systems to accept non-SMS/PSTN based authentication channels with minimal disruption.

- We believe that Verifiable Credentials should be considered as a recommended path forward to reducing switching costs into new forms of digital format-based authentication with improved security profiles.
- Additional verification is often helpful. For example, an important case in healthcare is to verify an insurance ID where the incentive is getting paid. There may be a subtle difference between verification of the identifier and authentication of the identity. Verifiable Credentials provide means to make this distinction.

Security and performance capabilities (e.g., presentation attack detection/liveness testing) for biometric characteristic collection to support Identity Assurance Level 2 remote identity proofing in the areas of identity evidence verification (physical/biometric comparison) or binding of authenticators.

- The use of biometric characteristics in conjunction with Verifiable Credentials and Decentralized Identifiers has not yet been fully explored. It has significant user privacy concerns that must be appropriately addressed prior to issuing community responses. Progress on the PING Self-Review for privacy in the DID Working Group can be found here. There is currently no specific work item for biometrics and Verifiable Credentials or Decentralized Identifiers at W3C CCG.
- Elsewhere in the decentralized identity community, during Rebooting Web of Trust 6, community members have created a draft of their approach to biometrics.

Capabilities and innovative approaches for remote identity proofing to achieve equivalent assurance as in-person identity proofing.

- No comments at this time.

Security and privacy considerations and performance metrics for the use of behavioral characteristics as an authentication factor.

- No comments at this time.

Use of dynamic knowledge-based information for identity verification.

- No comments at this time.

Capabilities to meet Federation Assurance Level 3 (see SP 800-63C FAQ C03).

- No comments at this time.

Capabilities and security considerations for verifier impersonation resistance (see SP 800-63B FAQ B04).

- Verifiable Credentials can enable a way for verifiers to authenticate themselves to a credential holders prior to presentation.
- Decentralized Identifiers with the appropriate authentication flows can allow credential holders to establish authenticity of the verifier.

Additional controls and mitigation to address the ongoing evolution of threats such as phishing and automated attacks.

- The DIDComm messaging protocol is being designed with consideration of ways to mitigate automated attacks by increasing the cost of attack, such as in this issue thread. We believe it should be considered as a tool to address phishing and automated attacks.

3. Comments by Document §

3.1 Document 800-63-3: Digital Identity Guidelines §

3.1.1 General Comments §

- The rules should clarify how the guidelines interface with trust frameworks that develop (for example, in a particular industry or domain and which some government agencies may wish to be apart), particularly in light of the increasing interaction between public and private sector.
- The guidelines could address issues regarding a relying party's right to rely. This might include, for example, a relying party's right to rely on an identity credential generally or rely on credentials issued under a certain trust framework.
- NIST could ensure that the rules do not discriminate among IdM system models by including the concept of IdM system neutrality. Because (as the current version recognises at the beginning) there are many different ways of conducting online identity transactions (e.g., single identity provider (IdP) systems, federated (multiple IdP) systems, user controlled/user centric systems/self-sovereign systems, hub systems, DLT systems, etc.), it is important that the rules do not require or assume a particular approach to the identification and/or authentication processes, or the system that delivers them. The guidelines should consider ways to ensure that Rules do not (regardless of the introductory disclaimers made) imply and/or require a certain system model.
- The Rules do not comment on standard allocation of liability. This is likely deliberate – eg. due to the public sector focus of the rules, or diversity of IdM systems such that it would be inappropriate to impose a one-size-fits-all approach. However, liability may be addressed in trust

frameworks. In many cases, private sector digital identity participants rely on attribute assertions from third parties, such as national IdM systems or other government databases (e.g., DMV). Since government IdM systems are often viewed as authoritative, they will not typically accept any liability for errors. Therefore determining who bears the loss in the case of errors in government supplied information is vital. The rules should address ways in which these obligations and liability allocation might be appropriately resolved.

- The NIST Guidelines could set out a process for certifying Trust Framework bodies for certain use-cases/communities which meet NIST guidelines.
- (Abstract) “These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose.” – As above, federal agencies are likely to increasingly interact with a more diverse identity eco-system moving forwards which will include customers who have been issued and wish to reuse identity credentials issued by non-federal agencies. The guidelines should address this reality and take into account models other than the federated approach.

3.1.2 Comments by Section §

Section 2 “This recommendation also provides guidelines for credential service providers (CSPs), verifiers, and relying parties (RPs)”

The framing throughout the rules (for example, the roles) fits/assumes the traditional IdM system model. IdM system models are undergoing a variety of changes and experimentation, raising concerns that using this list of obligations is based on an old model, that may not fit newer IdM systems and/or may unduly inhibit further experimentation.

Section 4.1 “The digital identity model used in these guidelines reflects technologies and architectures currently available in the market”

Some SSI technologies are in market – are the guidelines intended to cover SSI technologies?

“When a claimant successfully demonstrates possession and control of one or more authenticators to a verifier through an authentication protocol, the verifier can verify that the claimant is a valid subscriber. The verifier passes on an assertion about the subscriber, who maybe either pseudonymous or non-pseudonymous, to the RP”

In SSI, the role of the verifier is not required – or rather it is replaced by digital wallet component that acts on behalf of the subject.

Section 4.1 Figure 4-1

This is only one type of digital identity model – it is not representative of non-federated models.

Section 4.3.2 "A credential is stored and maintained by the CSP, though the claimant may possess it"

Why isn't the credential is stored where the user chooses – eg in the user's digital wallet and backed up.

Section 4.4 "Overall, SP 800-63 does not presuppose a federated identity architecture"

The roles depicted and language used do predicate a federated model. It would be difficult to adopt an SSI model AND adhere to the NIST digital identity guidelines.

The section sets out the benefits of a federated architecture over a siloed one, but there is no reference to or comparison to a decentralised model.

Section 4.4.1 Assertions "An RP trusts an assertion based on the source, the time of creation, how long the assertion is valid from time of creation, and the corresponding trust framework that governs the policies and processes of CSPs and RPs. "

NIST could clarify how trust frameworks interface with these guidelines.

"Examples of assertions include: (SAML, OIDC, Kerberos tickets)"

Verifiable credentials can also be containers for assertions.

Table 5.3 Federation Assurance Levels "FAL1: permits the RP to receive a bearer assertion from an identity provider (IdP). The IdP must sign the assertion using approved cryptography."

Can the digital wallet be the IdP in this context?

Section 6.1 "...more information on whether an agency can federate is provided in section 7"

What about more information on self-federation?

3.2 Document 800-63-A: Enrollment and Identity Proofing §

3.2.1 General Comments §

- No comments at this time.

3.2.2 Comments by Section §

Section 4.1 Process Flow "The CSP validates the information by checking an authoritative source"

What if the information an applicant receives from the authoritative source is already signed by them? Eg. in SSI where a credential is cryptographically signed by the issuer and does not need to be validated by a CSP for a relying party to rely on it.

Section 4.4 Identity Assurance Level 2

The framing assumes that a CSP is present, when this role is not always necessary – eg. if the individual has their credentials issued to them directly by the issuer, they can present these to a relying party without the need for a CSP to be involved.

Section 4.4.1.6 Address Confirmation

If a utilities company provided a proof of address credentials (eg. because internet was connected at the address and paid for by the applicant), would this be an acceptable form of address confirmation?

Section 5.3.2

Large focus on Knowledge Based Verification requirements – what about guidelines for "something you have"?

Section 8.1.1 Social Security Numbers "...Overreliance on the SSN can contribute to misuse and place the applicant at risk of harm, such as through identity theft. Nonetheless, ..."

For some use cases, when Privacy concern is high, one time use of Decentralized Identifiers or derivative artifacts may be considered for use as unique alternative identifiers to the SSN. For further privacy, the pairwise DID identifiers can be used. The DID is meaningless by itself, but globally unique. It has the potential to mitigate correlation risks.

Furthermore, DID-based systems should prevent DIDs from being used for authentication, so the harm in public exposure is reduced. The same DID has the potential to be used across systems, agencies, and organizations without compromising its security and privacy properties.

We refer to the following item:

1. DHS RFP: Preventing Forgery & Counterfeiting of Certificates and Licenses (Release 2) SVIP OTS Call 70RSAT19R0000002/0001 Scenario I: Alternative Identifier to the Social Security number. This RFP is seeking alternative identifier to SSN.

3.3 Document 800-63-B: Authentication and Lifecycle Management §

3.3.1 General Comments §

- We prioritize the idea of authentication based on something you have rather than something you know
- Innovations in DID, especially ephemeral DIDs, would add privacy-preserving properties.

3.3.2 Comments by Section §

Section 9.3 Use Limitation "...CSPs may have various business purposes for processing attributes, including providing non-identity services to subscribers. However, processing attributes for other purposes than those specified at collection can create privacy risks when individuals are not expecting or comfortable with the additional processing."

In some use cases, Selective Disclosure and Zero-Knowledge Proofs with Verifiable Credentials can be leveraged when individuals wish to utilize information minimization.

3.4 Document 800-63-C: Federation and Assertions §

3.4.1 General Comments §

- The guidelines refer to the IdP – the guidelines should clarify whether an SSI based mobile wallet could be the 'IdP' or 'federator' in this context.
- Could consider including a new mechanism for federation that is based on SSI or decentralized technology

3.4.2 Comments by Section §

Figure 5

Figure 5 talks about federation as a three party relationship which includes an IdP – again, the guidelines should clarify the terminology on what amounts to an IdP and whether this could be a digital wallet/software agent acting on behalf of the user.

5.1

Assumes a centralized approach, could benefit from a web of trust federation model?

- Enterprise consortia, NIST Blockchain Taxonomy Guide, EEA, ERC725
- DIF and OpenID collaboration on SIOP-related issues
- Digital Credentials Consortium
- eSSIF / EBSI