From: Sam Smith
Sent: Friday, July 31, 2020 2:02 PM
To: dig-comments-RFC <dig-comments-rfc@nist.gov>
Subject: Comments on Digital Identity Guidelines RFC

To whom it may concern.

As Chairman of the Board of Trustees of the Sovrin Foundation, I suggest that NIST should consider the body of work initiated by the Sovrin Foundation and its larger community https://sovrin.org/library/ . This has resulted in work in the Linux Foundation's HyperLedger's Indy, Aries, and Ursa projects (https://www.hyperledger.org /use/ hyperledger-indy, https://www.hyperledger.org/use/ursa, https: //www.hyperledger.org/use/aries) as well as work on projects within the Decentralized Identity Foundation https://identity.foundation and the W3C Decentralized Identifier (DID) and Verifiable Credentials standards.

In my opinion the most important work relevant to the NIST Digital Identity Guidelines is a recent project within DIF that is building an identity system security overlay for the internet that will provide a universal trust spanning layer. This overlay is based on generalized self-certifying identifiers that provide a cryptographic root-of-trust instead of a dependency on assumed trusted entities as is the case for the DNS/CA system. This cryptographic root-of-trust enables full end-verifiability of all operations on identifiers. This will fix the major security vulnerabilities of DNS/CA which is trust on the operational security of intervening infra-structure. The name of this project is KERI for Key Event Receipt Infrastructure. I am the principle originator of this project. Complete details of the system theory are provided in a 134 page white paper which may be found on arXiv. https://arxiv.org/abs/1907.02143. The latest version of the paper may be found on GitHub here. https://github.com/SmithSamuelM/Papers/blob/master/whitepapers /KERI_WP_2.x.web.pdf https://github.com/SmithSamuelM/Papers/blob/master /presentations/KERI2_Overview.web.pdf . KERI is the culmination of several years of work in the decentralized or self-sovereign identity space starting with the original work I began in early 2015 that became a major impetus behind the creation of the Sovrin Foundation and its a liated projects on (SSI) self-sovereign or decentralized identity.

Noteworthy is the KERI does not depend on totally ordered distributed consensus ledgers. Although KERI may employ ledgers when useful, it does not require them. This gives KERI performance scalability and allows it to operate in high performance data streaming applications. KERI employs a novel pre-rotation future commitment on its keys that is post-quantum secure. Moreover the associated identifiers are fully portable across

computing infrastructures and fully agile across cryptographic operations thus giving the KERI the potential as a truly universal trust spanning layer.

Thank you for your consideration.

I am available to answer questions.

Samuel M. Smith