Generalizing Secure Scuttlebutt for Data Integrity

by Charles E. Lehner, Spruce Systems, Inc., New York

A proposal for generalizing or applying the Secure Scuttlebutt system to DIDs and Data Integrity.

Abstract

Secure Scuttlebutt (SSB) is an peer-to-peer communication protocol, mesh network and self-hosted social media ecosystem. While SSB has proved to be viable for an ongoing decentralized community, the protocol was started before and continued to evolve in parallel to the work on W3C Decentralized Identifiers (DID). SSB's account system is based on asymmetric keys and shares similar characteristics with very simple DIDs. This paper describes how DIDs can help to improve the SSB protocol which will help to move the SSB and DID community closer together.

Intro

Secure Scuttlebutt (SSB) is a peer-to-peer database with free-libre/open-source social network applications. SSB accounts are identified by a keypair and cryptographic signature type. SSB accounts publish messages signed with the account's keypair. SSB messages are identified by a cryptographic digest (hash). Each message links to the previous message by its hash, forming an append-only log structure called a feed. Public deployments of Secure Scuttlebutt use Ed25519 keypairs and signature, and SHA-256 for the message hash algorithm. SSB messages are JSON. Serialization of SSB messages for hashing and signing predates JSON Canonicalization Scheme. The hash of a SSB message is computed using a custom binary serialization.

Decentralized Identifiers (DIDs) are a syntax and data model for identifiers that can be used to cryptographically authenticate messages. DIDs are a W3C Recommendation as of this writing. DIDs share some functionality with SSB account/feed identifiers. In SSB, an account ID (feed ID) encodes a cryptographic public key. A DID resolves to a DID document containing zero or more public keys. A SSB ID is therefore analogous to a `did:key` DID. However, SSB messages are expected to exist in an SSB feed (append-only list of messages), conforming to a specific message format; while DIDs may sign many kinds of messages (e.g. Verifiable Credentials, Verifiable Presentations; Data Integrity messages, JSON Web Tokens) in any sequence.

SSB has proved to be viable for an ongoing decentralized community with sustained activity (from 2014/2015 to 2022 as of this writing). Its limitations/challenges relate to onboarding, resource use, peer discoverability, and topic- or group-based content discoverability/distribution.

Proposal

TBD: questions that need to be addressed in the final paper (during/after RWOT):

- Can it be useful to generalize or modify SSB to use DIDs for account IDs?
- Why and how DIDs can help with certain issues SSB has today?
- How to represent SSB accounts as DIDs?
- How to fit DIDs and their decentralized PKI into SSB?
- How to address backward compatibility?
- How may new SSB protocol developments (e.g. feed linking, private groups, and lipmaa links) interact with use of DIDs?
- What could interoperability look like in a SSB-like environment with many DID methods? what new affordances may be needed?
- Can existing SSB message formats continue to be used, or would other DID method communities prefer other message formats (e.g. ActivityPub)?
- Are SSB's tradeoffs with regards to immutability acceptable?

Conclusion

TBD: during RWOT