Advanced DIDComm Messaging

By: Karim Stekelenburg (Animo Solutions) – karim@animo.id **Date:** 18-07-2022
Version: 0.1

Introduction

DIDComm is a promising technology. Although it finds its origin in the space of self-sovereign identity and is primarily used for the exchange of verifiable credentials and presentations, its potential stretches far beyond. One application where DIDComm has potential is chat.

Why?

DIDComm provides a secure and private communication channel based on decentralised identifiers (DIDs). One can leverage this nature of DIDComm for application specific use cases, by writing protocols atop of DIDComm. Although it is already possible to exchange simple text messages over DIDComm by using the basic-message protocol, in order for DIDComm to provide a potential replacement for commonly used chat protocols like WhatsApp (Extensible Messaging and Presence Protocol (XMPP)), Telegram (MTProto), or Signal (Signal Protocol), it needs to support modern chat features we use everyday.

Research questions

This proposal evolves around extending DIDComm with missing features compared to aforementioned chat apps and protocols. All research questions are with regards implementing the following set of features:

- Hyperlinks
- Group chat
    - Administrator roles
    - Out-of-band invitations
- Read receipts
- Named threads
- Message replies and reactions
- Message forwarding
- Message editing
- Time sent / time delivered metadata
- Time-sensitive messages (expiration)
- Attachments

Resources

- DIDComm
- Basic Message Protocol