Dear team, by the end of this time, you should have written an abstract which is:

- A self-contained text, not an excerpt from the paper
- Be fully understandable on its own
- Reflect the structure of your larger work

Here are some questions to help you get aligned on the work ahead:

Purpose: Why does this artifact exist? What makes it important?
Audience & Impact: What is it aiming to do & for whom?
Keywords: What are some keywords associated with the world of this artifact?

& some examples from past events:
(from Amira 1.0.0)[1]

> *This paper began as a collaborative project at the fifth Rebooting the Web of Trust[1] workshop, held in Cambridge MA in October 2017. We reinterpret Christopher Allen's Rebooting the Web of Trust user story,[2] through the lens of the Information Lifecycle Engagement Model (described in Appendix A). We present a human-centric illustration of an individual's experience in a self-sovereign, decentralized realization of the Web of Trust as originally conceived by Phil Zimmerman for PGP.[3]*
>
> *In our scenario, Amira is a successful programmer working in Boston at a prestigious multi-national bank. Outside of working hours, Amira wants to give back to her community by writing software that matters. On the advice of her friend Charlene, Amira joins RISK, a self-sovereign reputation network that connects developers with projects while protecting participants' anonymity, building reputation, and sending & receiving secure payments.*

(From Introduction to DID Auth)[2]

> *The term DID Auth has been used in different ways and is currently not well-defined. We define DID Auth as a ceremony where an identity owner, with the help of various components such as web browsers, mobile devices, and other agents, proves to a relying party that they are in control of a DID. This means demonstrating control of the DID using the mechanism specified in the DID Document's "authentication" object. This could take place using a number of different data formats, protocols, and flows. DID Auth includes the ability to establish mutually authenticated communication channels and to authenticate to web sites and applications. Authorization, Verifiable Credentials, and Capabilities are built on top of DID Auth and are out of scope for this document. This paper gives on overview of the scope of DID Auth, supported protocols and flows, and the use of components of the DID Documents that are relevant to authentication, as well as formats for challenges and responses.*

---

[1] https://github.com/WebOfTrustInfo/rwot5-boston/blob/master/final-documents/amira.md
[2] https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/did-auth.md