**Minutes of Meeting #4 of Linux Foundation IAM Project (Draft)**

Meeting Date: 12 July 2022

Attendance:

|  |
| --- |
| Chris Buchanan, MITRE  Jim St. Clair, Linux Foundation |
| Jim Schoening |
| Casey Rock, US Army Futures Command |
| Jeanae Clark, Booz Allan Hamilton in support of US Army  Mark Jensen  Marvin tried but couldn’t join due (Jim Schoening had tech issues and started 20+ minutes late)  Iain Henderson was unable to attend but met with J Schoening prior.  A transcript of this meeting is posted at <https://github.com/I-AM-project/Overall-Project-Documents>    **Agenda:**  1. Review updated Goals and Objectives (posted at github.com/I-AM-project) --Jim Schoening  2. IAM-Project Testbed (Sneak Peak of Wallet with iPDS) -- Jeanae and Casey  3. Commitments for demonstrations  -- Jim Schoening  4. Status on seeking Aries collaborators -- Jim Schoening  5. Key choices: a: Bedrock b. KERI c. Aries d. Other  -- Casey and all  6. Next steps / Growing the team -- Jim St. Clair and all |
|  |
| **Minutes:** All agenda items were covered, with the following significant comments.  Casey and Jeanae showed the testbed.  Chris provided the following feedback:   1. The public key that is out there for people to see is not related to the key you're using for encryption, because the more you use it, the more vulnerable it becomes, and the public keys are the hardest to rotate. 2. So what you'd want to do is use that for proof of control right? Basically, for identity binding to say yes, this is me and I can prove it and then what's on the Ledger is functionally how you know that the person you're talking to is the person you intended to talk to. 3. What you can do is do a key swap. You can do a public key swap directly between you and the platform and then create an asymmetric key that then represents your relationship with that platform. 4. That's what you call a pairwise sidonius? relationship, right? So now you have the ability to prove to the platform that you're the same person that they establish that relationship with, and then all the data is still signed. And you can you can prove control over the signed key and you've got the identity binding. So, they know you. You're not an interloper. You're not a man in the middle or something like that. And you have the ability to prove control over the key. 5. Recommend Casey attend Internet Identity Workshop in Nov in San Jose, CA. 6. Self signing works primarily for identity binding, but also become a communications channel that others can’t track. 7. There will absolutely be a market for for know your customer level identity proofing that is portable. 8. To verify paper documents, a notary public could do that. These could be used for zero knowledge proofs. 9. We need VCs to be insurable assets to cover fraud. 10. when you settle on an architecture that you go through the trust over IP process called a tip which which is functionally a registration of your use case 11. Trinsic is probably the most mature SSI wallet platform for custodial wallets. Maybe talk to Riley at Trinsic. 12. What do I do when I switch devices is so nontrivial that having that Edge Wallet is not tenable at the moment until that is figured out.   Commitments for tech demos include:   1. LF Hyperledger Identity Implementers WG (date TBD) 2. Mortgage 3. Pharmacy Operations   Outreach: Jim Schoening reached out to leaders of the Aries Javascript WG, who agreed to meet. He agreed to continue to reach out to other Aries groups or adopters to gauge their interest in a PDS for their cloud agents/wallets.  There was consensus to not attempt to reinvent the wheel on VCs, but rather to make use of the work of others. This will allow us to focus on our unique contribution of an integrated PDS  Jim St. Clair commented: The mortgage use case is very similar to the Didymium use cases of life and health insurance.  Respectfully distributed and post on 12 July 2022 by James Schoening, [james.schoening@ieee.org](mailto:james.schoening@ieee.org). Please send edits to these draft minutes. |
|  |
|  |
|  |