2021-12-02 TATF Meeting Notes

Meeting Date

- 02 Dec 2021
  - **NA/EU 07:00-8:00 PT / 15:00-16:00 UTC**
  - **APAC 1:00-2:00PM PT / 21:00-22:00 UTC** **<== NOTE THE NEW TIME**

Zoom Meeting Link / Recording

- AM (US + EU) meeting - https://zoom.us/rec/share/rgJRp_O_KzSjlScg1q9uLudaABEzgbxMGqyPgasXxmPY5K_evvoiROEbUUFXdcgT.rGt-A1VnkNv6Zh6G?startTime=1638457710000
- PM (APAC+US) meeting - https://zoom.us/rec/share/W345sXSd89q_gQS4_P5E4wS4ZbqY6CtZcrGX5Tu_HT1avBXDHnewgTaz0WIrDBcY.LG30OODnbvT8w4x5?startTime=1638478790000

Attendees

NA/EU

- Drummond Reed
- Darrell O'Donnell
- Vikas Malhotra
- Phil Feairheller
- Adrian Gropper
- Samuel Smith
- Antti Kettunen
- Daniel Bachenheimer
- Isaac Henderson
- Kevin Griffin

APAC

- Drummond Reed
- Darrell O'Donnell
- Jo Spencer
- Tim Bouma
- Wenjing Chu
- Scott
- Samuel Smith

Main Goal of this Meeting

Input from Dr. Sam Smith ; determine what types of diagrams we will need and who is doing consolidated drafts of each; decide on holiday meeting schedule.

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
5 min	• Start recording • Welcome & antitrust notice • Introduction of new members • Agenda review	Chairs	• **Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws. Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* • New Members: Adrian Gropper

5 min	Review of previous action items	Chairs	☑ ACTION: ALL — Over the US Thanksgiving break, think about what other types of diagrams we need in addition to a protocol stack diagram, then if possible add your suggested version of other diagrams to the ToIP Protocol Stack Diagrams slide deck. ☑ ACTION: ALL — review the outline of the ToIP Technology Architecture Specification draft and identify sections where you are interested in contributing text.
15 mins	Input from Dr. Sam Smith	Samuel Smith (if able to attend)	Discuss Sam's thoughts on protocol layering and where KERI protocols, serialization formats (such as CESR), and KERI key management would fit. • Sam felt it was very important to "unpack" the trust spanning layers • To do this, he had to go over the PAC Theorem - see slide screenshots #1-#6 below. • It means that authenticity and confidentiality and privacy • KERI layers it: authenticity, then confidentiality, then privacy ◦ Privacy is achieved by using a combination of legal liability on participants • That could be two stacks - one for data in motion and one with data at rest • Antti Kettunen pointed out that you can link a transaction to one or more verifiable credentials in order to prove authenticity • Sam pointed out that can work, but it is based on reputational trust, because they are trusting recourse • Legal systems only recognize reputation associated with legal identity • The key conclusion from this is that we need to look at the layering of authenticity and confidentiality and privacy • Sam pointed out that we have the communication stack and the priority stack • Sam said, "The reason this is difficult is that security has always been a bolt-on, but if you want to make it critical." • Darrell pointed out that we need to decide about the three factors. And all ZKP-system will not provide authenticity. • Phil Feairheller said that different priorities work for different use cases. • Antti Kettunen thanked Sam for bringing the PAC Theorem.

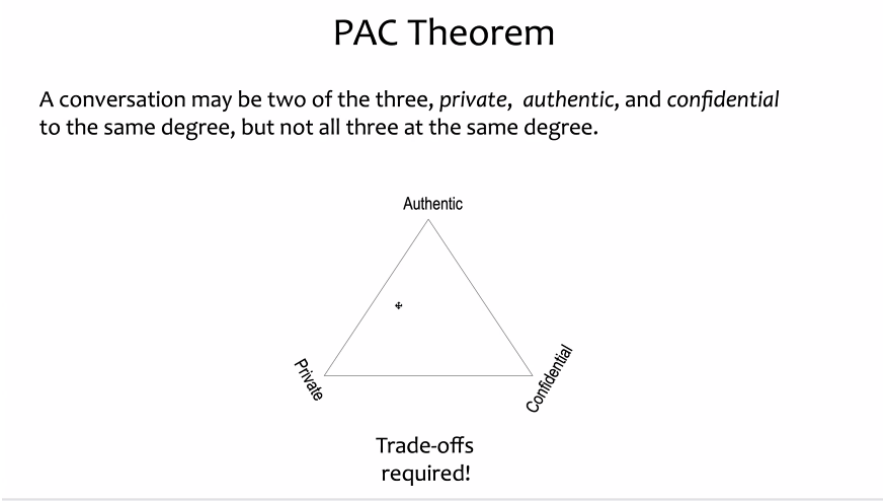
5 min	Square white paper	Drummond Reed
		
		Jo Spencer
			Square (where Daniel Buchner recently left Microsoft to join) put out this white paper called tbDEX: A Liquidity Protocol v0.1. Quote:
			> *At its core, the tbDEX protocol facilitates the formation of networks of mutual trust between counterparties that are not centrally controlled; it allows participants to negotiate trust directly with each other (or rely on mutually trusted third-parties to vouch for counterparties), and price their exchanges to account for perceived risk and specific requirements.*
			• Drummond Reed noted that it is entirely based on DIDs and VCs, but it doesn't really explain anything about the details of the tbDEX protocol
			• Jo Spencer said that his background is in payments, and so this proposed protocol is "right in his wheelhouse"
			  ◦ The key problems in payment protocols are around trust—if you solve that, the payment piece is relatively easy
			  ◦ So Jo was excited when he saw this proposed protocol in terms of its scope.
			  ◦ But then he felt that it didn't actually fix the problem—it starts, but then it doesn't finish.
			• Tim said that first, we saw money move away from the government space, and now we're seeing identity moving away from the government space
			  ◦ The Bitcoin lightning protocol is a good example.
			  ◦ Tim believes now that digital assets like Bitcoin are starting to become legitimized
			  ◦ This is bringing the decentralized ingredients that are necessary: DIDs, DLTs, smart contracts
			  ◦ This means that you can create a system that works totally outside of the domain of the state
			  ◦ What excited Tim about the paper was that it brought in DIDs for peer-to-peer interactions that can still be secure, and to exchange VCs for trust, and now to trade with one another
			  ◦ If we can formalize this is the work we're doing here, then we have the potential to put together a policy framework for it
			  ◦ It will very interesting geopolitically to see how this plays out.
			• Jo and Tim felt that CBDCs are going to have to co-exist with non-state currencies
			  ◦ Tim feels that CBDC's won't be that different than stable coins
			  ◦ Some of the assumptions we've had post WW2 are changing.
			  ◦ 10+ year play
			• Sam:
			  ◦ Raised "reputation economy" - where you ditch money and move to exchanging value.
			  ◦ in-person requires less trust in the system as you're in person - but going remote requires reputation
			• Jo - the tbDEX tries to do too much (Darrell agrees)

20 mins	Technical architecture diagram types	All	Discuss/decide what different types of diagrams we need for the ToIP Technology Architecture Specification. See this Medium article for more about types #2 thru #6 below. 1. Protocol stack diagram 2. Application architecture diagram 3. Integration architecture diagram 4. Deployment architecture diagram 5. DevOps Architecture diagram 6. Data Architecture diagram NEEDS • Verifiable Credentials Exchange - this is where things started, so not showing detail on it would be odd. WC: another fleshed-out protocol besides credential exchange. Perhaps payments? • is Streaming data the oddball (others are messaging-esque)?
10 mins	Possible post-holiday special meetings	All	• Daniel Hardman will be returning to Utah over the holidays • Drummond Reed is thinking of making a trip down to Utah to meet with Daniel, Samuel Smith, Phil Windley, and other architects to talk about DIDComm, KERI, and the ToIP Technology Architecture Specification

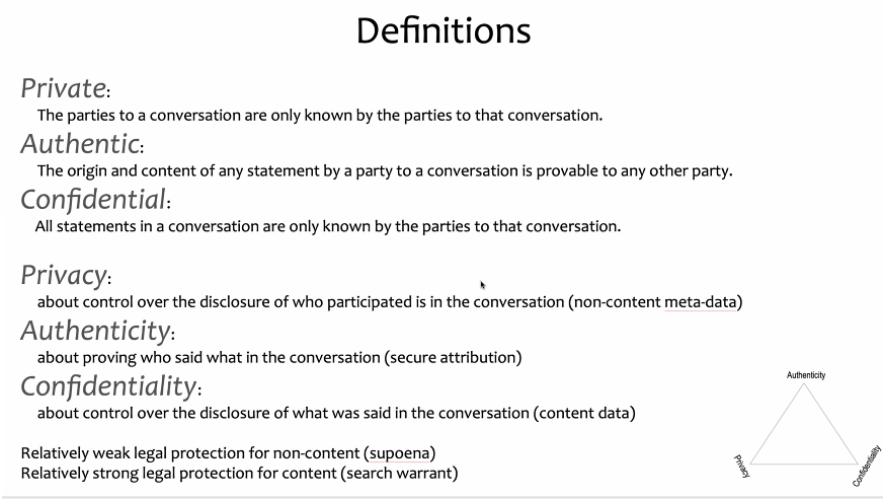
5 mins	• Review decisions/action items • Planning for next meeting	Chairs	Holiday meeting schedule: • No meetings Dec 23 or Dec 30th • Resume meetings Jan 6 2020 ACTION ITEM: ALL to review and consider Sam Smith's slide deck about the PAC Theorem. ACTION ITEM: Review the Square white paper on the tbDEX: A Liquidity Protocol v0.1.

Screenshots/Diagrams (numbered for reference in notes above)

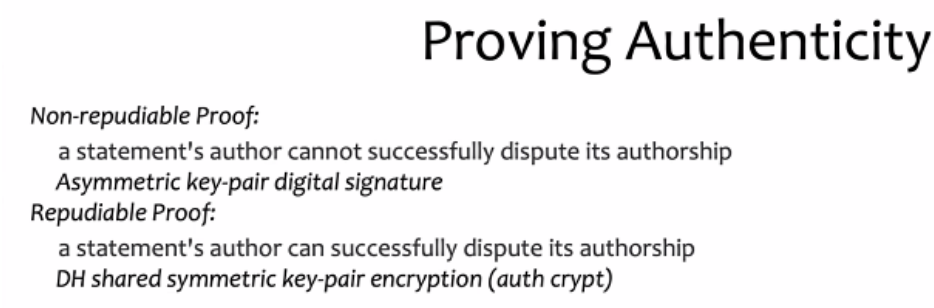
#1



#2



#3



#4

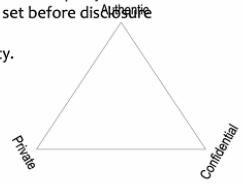
Trade-offs

Private:
The parties to a conversation are only known by the parties to that conversation.

Authentic:
The origin and content of any statement by a party to a conversation is provable to any other party.

Confidential:
All statements in a conversation are only known by the parties to that conversation.

Non-repudiation means any party to conversation can proof to any other party exactly what was said by whom.
This means that technologically there is no way to prevent disclosure by any party to some third party.
We can incentivize confidentiality by imposing a liability on the parties to the disclosure set before disclosure occurs.
Enforcement of that liability will usually necessarily violate privacy but not confidentiality.
Real world value often requires transitivity.
Transitive value transfer will violate complete privacy.



#5

Layering

A communication system can layer the different properties in different orders thereby imposing a priority on each property.

Authenticity
Confidentiality
Privacy

Decisions

- **DECISION: The Technology Architecture TF will NOT meet on Dec 23 or 30. Meetings will resume Thursday Jan 6 2022.**

Action Items

- [ ] ACTION ITEM: ALL to review and consider Sam Smith's slide deck about the PAC Theorem.
- [ ] ACTION ITEM: Review the Square white paper on the tbDEX: A Liquidity Protocol v0.1.