2019-06-12-Notes

Agenda

Attendees

Name	Reference
Vipin Bharathan	dlt.nyc
Luca Boldrin	Infocert
Steve Magennis	
Todd Gehrke	Luxoft
Ajay Jadhav	AyanWorks
Ravi Agrawal	
Shinzi Satou	
Jim Mason	DMX
Sid	
Nitin Agarwal	Gio
Drummond Reed	Sovrin, Evernym
Andres "Dre" Bonifacio	SymPact, SI-SIG

There were two great presentations. Thanks to Todd Gehrke for his contribution in recording the call.

Audio

Video

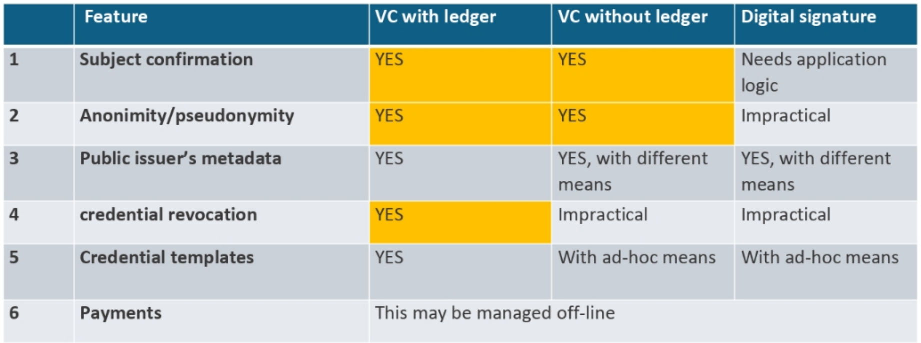
Do we need dlts or blockchains to implement SSI or DIDs?

By Luca Boldrin

What is the real value that the ledger brings to SSI, this is what he expects to answer in the presentation.

Some points that he made:

- This is the result of his long discussion with his colleagues and may be biased as he works for a CA company.
- Luca outlined the gist of how PKI works including the fact that a list of CAs were anchored on the Browser and in applications like the Adobe Trust List where it is used for digital signatures.
- He outlined how the standard SSI case works in the exchange of verifiable credentials for Alice (S) in the context of an Issuing Party (IP) Faber University, a Relying Party (RP) Acme Hospital. Removing the need to create a channel between the IP and the RP.
- The trust framework can involve digital signatures and a domain specific trust framework; for the RP to trust IP. Digital Signature based approach.
- First case is through the use of CAs on a trust list who sign the IPs certificate (which includes their public key) and which then leads us to trust the credential since it has been signed privately by the IP using their private key.
- Luca went through a VC based approach that can use a ledger and contrasts it with a ledger based approach.
- Then Luca demonstrates using a matrix the comparison of a non-Ledger (CA) based approach to a ledger based approach contrasting with the Digital Signature based approach. Best captured in the following diagram, where revocation is seen as a distinguishing feature of a ledger based approach.



	Feature	VC with ledger	VC without ledger	Digital signature
1	**Subject confirmation**	YES	YES	Needs application logic
2	**Anonimity/pseudonymity**	YES	YES	Impractical
3	**Public issuer's metadata**	YES	YES, with different means	YES, with different means
4	**credential revocation**	YES	Impractical	Impractical
5	**Credential templates**	YES	With ad-hoc means	With ad-hoc means
6	**Payments**	This may be managed off-line		

-
- Questions and comments followed: Jim Mason suggested that another row in the matrix should be Auditing, Luca seemed to agree.

References:

Preliminary slides

The Consent Layer in the India Stack by Ajay Jadhav

Although Ajay only had a short time, he ably presented on the consent layer, which drew a host of questions on the various aspects. We worked on an extension of about 10 minutes to the call due to demand and interest from the community. Hopefully he will present this architecture in greater detail in a later call.

Although the India stack has had many detractors due to its reliance on the Aadhaar number, the most widely deployed national ID, the India Stack continues to evolve.

Most of the criticism is related to the overreach and surveillance capabilities of the system; however the privacy layer and protection for individual entities are being back-filled through a series of supreme court rulings and bills. See the reference section for Personal data protection bill.

Data classification from personal, generalized data to derived data (covered in detail in the slides) and what is protected and the drivers behind it.

The Digital Locker being is an important element of the India stack, the consent to share has to be captured along with data issued as well as data shared. The Locker is centrally created, but in control of the user who chooses to add items to it and protected by regulation.

There is a short section on the overall architecture of the consent layer (which is not yet in production)

The slides from iSpirit also contain a number of use cases in the Indian context.

Questions: the specifics of Indian Regulation for privacy protection from Steve Magennis which was answered by Nitin Agarwal and Ajay (see the references to bills below).

References:

India stack from medium

WHAT IS INDIA STACK?
https://indiastack.org/about/

Data Empowerment & Protection Architecture (DEPA)- Ajay's slides
https://www.slideshare.net/ProductNation/data-empowerment-protection-architecture-depa

Electronic Consent Framework
http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework v1.1.pdf

Data Protection Bill

https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf