Disposable or Ephemeral Identities

@robvank

The Self Sovereign Framework renegotiates power divisions

The Self Sovereign Framework renegotiates the power divisions between public institutions paid for by taxes, corporate actors paid for services, and citizens without whom both actors would not have a factual base for existence.

Self-Sovereign Identity is a win-win-win for all actors. It creates a small time out in which we can renegotiate our rights and our duties as responsible individuals in the different contexts of our everyday lives, taking care of our streets, neighborhoods, regions, and the planet.

Disposable identities are the antidote to continuous and real-time tracking and tracing of identified users. They break the one number one person relationshiop and are thus a fully new ontology.

Disposable identities are the antidote to continuous and real-time tracking and tracing of identified users. Instead, they operate via multiples of composable' attribute-based relational identities. Generated for each single interaction between user and service (or object and service) disposable identities are to be disposed of immediately after an event transaction.

With disposable identities, an enormous number of diverse applications can run on this ecosystem using a strict attribute-based solution, needing no full disclosure (of identity or social network ties) beyond the bare minimum: eg age, ability to pay for the service, legal compliance in terms of insurance and accountability. Digital services can be delivered to authenticated users without requiring the need for a single full set of identifying data on identity attributes to be shared.

Self-sovereign ID Standards

- The WC standard for SSID is the DID standard
  - https://www.w3.org/TR/did-core/
  - This is a persistent reusable identity for the individual
- W3C also has a Verifiable Credentials standard
  - The Verifiable Credential Data Model
  - https://www.w3.org/TR/vc-data-model/

- Disposable IDs takes this a step further by providing an SSID unique to a specific context
  - Disposable IDs make use of the W3C DID standard
  - The disposable DID may or may not make reference to an existing persistent DID
- Since Disposable IDs are context-specific, users can choose different trusted 3rd parties for different contexts
  - e.g. an automobile club or other association
  - e.g. a trusted person in the community (like a notary)

Original Proposal Outline

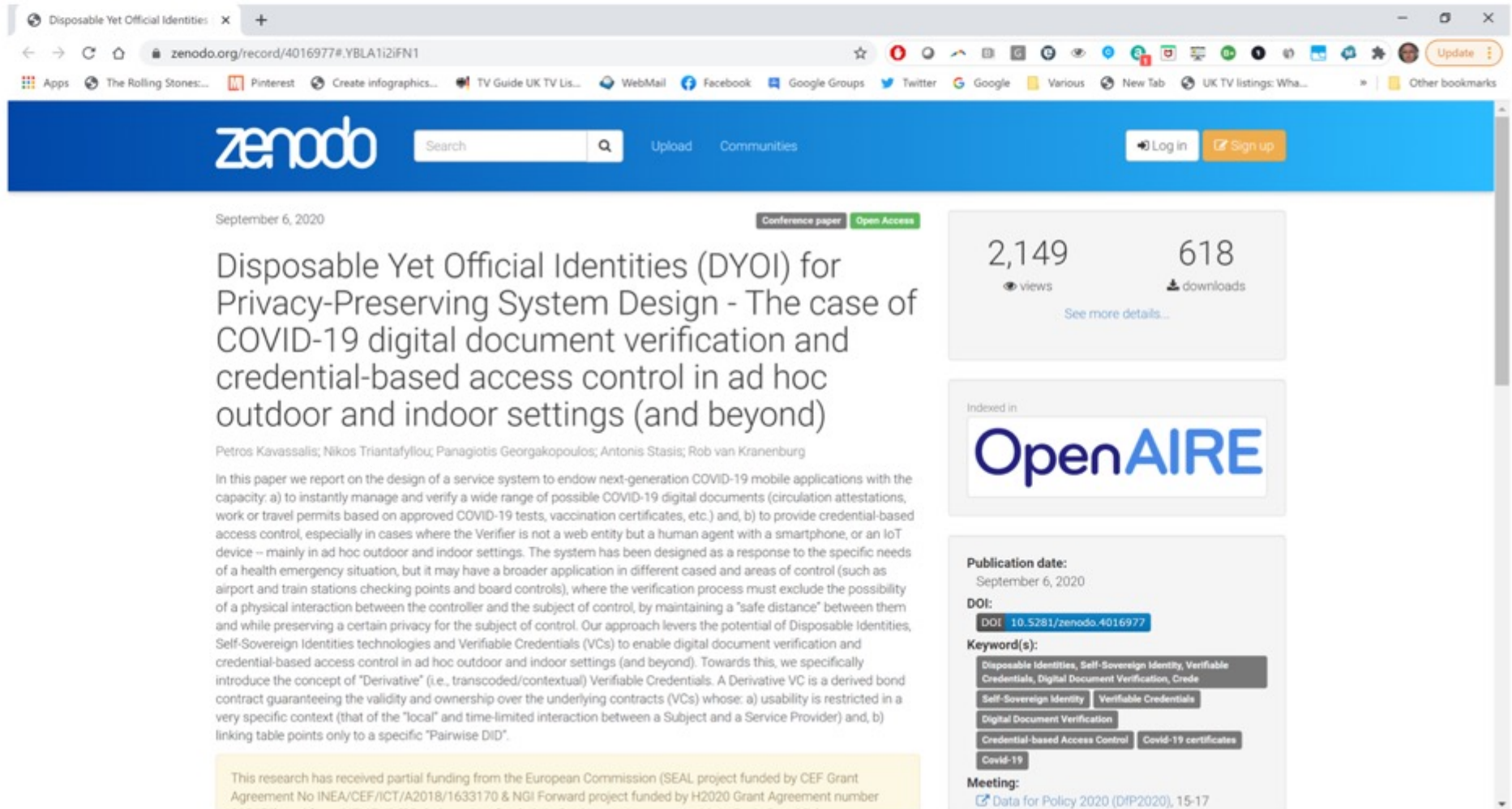
- This is a proposal for a digital identity management framework based on the concept of Disposable Proof of Identity.
- Disposable Proofs of Identity are made from domain and context-specific-specific personal data, and they are time-limited in scope.
- They should allow a subject to prove ownership of these data, without permitting anybody else to make (present or future) correlations between them and the subject's true identity.
- Essentially, a subject can generate many purpose-oriented “disposable” credentials, which are linked to different DIDs (W3C Decentralized Identifiers) over which a person has ownership or control.
- Only the subjects themselves can make the correlation between the different DID under their ownership, via a "verifiable presentation" (principle of unlinkability);
  - that means, if requested, a subject can create and present links between different Identities, or between a Disposable Proof of Identity and an "Official Identity" (Disposable Yet Official Identities).
- Disposable Proofs of Identity should be developed as Self Sovereign Identity-based Verifiable Credentials, in different forms and flavors
  - (including short-living tokens for one-time-use, a sort of "tiny" Disposable Proofs of Identity).
- In this sense, this proposal meets the objectives of the "Blockchain-based Identity Framework" proposed by ALASTRIA.

Contextual Trusted Third Parties

- Disposable SSID potential standard lets you choose a trusted 3rd party for a specific context
  - E.g. this car journey
- This means I can choose a trusted 3rd party appropriate to that context
  - E.g. all car journeys: I choose the Automobile Association that I belong to
- This means in turn that I could choose a trusted 3rd party for a specific kind of purpose
  - Clinic or my doctor for all health purposes
  - Automobile association for all my car-related purposes
- The ontology of purpose v context could be something to include in a potential standard?

Other DSSID Activities and Publications

- RFI: We want to know about any other work in this area
  - Example: Petros Kavassalis et al: https://zenodo.org/record/4016977#.YBLA1i2iFN1



Disposable or Ephemeral Identities RF extended : contact Mike Bennett mbennett@hypercube.co.uk

- forthcoming in The International Journal of Cyber Forensics and Advanced Threat Investigations (CFATI) co-authored with Gaëlle Le Gars.

In our connected world security and proof (evidence constituted in Verifiable Credentials (VC, W3C)) is distributed over what an individual can attest, what my objects tell about me (that is why AI = inferences from that data, are so important) and my behavior: “apply shaving foam” is a number in Coelition.org. It is clear that we can no longer isolate the notion of security as in securing devices or securing infrastructure. In this brief talk I sketch what we believe to be the end of a paradigm of a government model that has outsourced capabilities to the market. It is in the process of privatizing its last public capability: identity management. This is causing tremendous stress in systems, services, organizational procedures and individuals.

In short, Dfinity hopes that it will offer the first truly global blockchain network that runs at the top web speed with unlimited scaling features to support any volume smart contracts computation.

“If the IC succeeds at replacing legacy IT, there would be no need for centralized DNS services, anti-virus, firewalls, database systems, cloud services, and VPNs either,” noted Mira Christanto, researcher at crypto analytics platform Messari.

Dfinity proposes decentralization by introducing a unique consensus model dubbed as Threshold Relay, coupled with its Blockchain Nervous System to ensure algorithmic governance.

https://cointelegraph.com/news/how-did-internet-computer-icp-become-a-top-10-cryptocurrency-overnight