A Digital Yellow Card Using Decentralized PKI

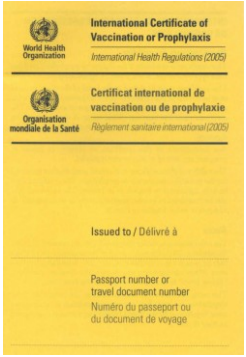
Stephen Wilson

Founder & Managing Director, Lockstep Technologies
swilson@lockstep.com.au

JUNE 2021 | #identiverse

Carte jeune
Digital challenges

- Copy resistance
- Provenance: proof of origin
- Interoperability
- “Identity”: avoid over-identification.



International Certificate of Vaccination or Prophylaxis

Ambulance chasing?

"While there earlier seemed no real use-case for a cross-border global identity system, immunity passports were seized upon as the killer use-case."

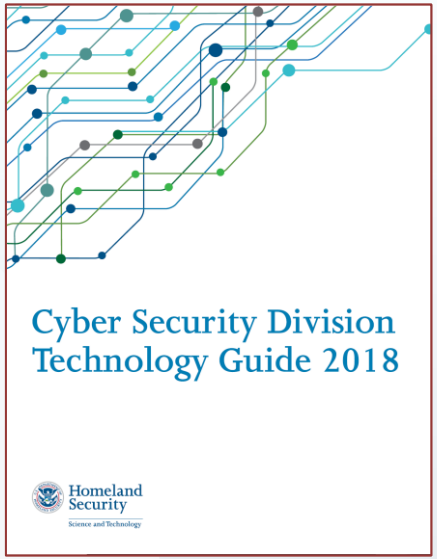
Harry Halpin, *A Critique of Immunity Passports and W3C Decentralized Identifiers.*

Unfortunately, a great many technology companies – especially from the digital identity and blockchain industries – seem to be taking advantage of the situation as an opportunity to advance their solutions and worldview. A number of consortia are racing to set standards.

Is this an identity issue?

- States register people differently
- Health authorities have processes for identifying vaccine recipients and keeping records
- Thin file individuals with little or no official identification are still dealt with
- NGOs find a way.

PoC: Mobile Device Attributes Validation (MDAV)

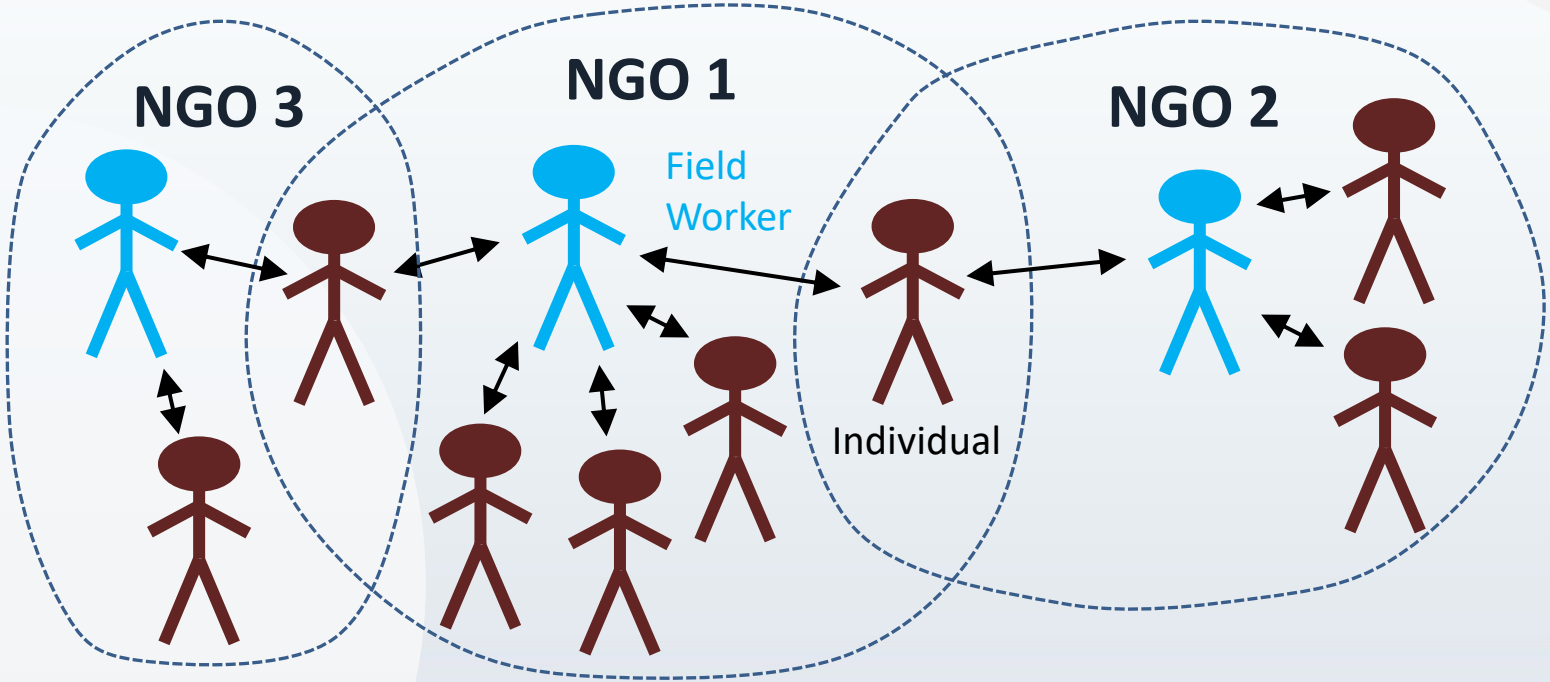


The detailed proposals in this presentation for digitised proof of vaccination are based on Lockstep Technologies' R&D of a mobile credentials wallet for emergency workers, carried out under contract for the Dept. of Homeland Security, within the Kantara Identity & Privacy Incubator (KIPI).

Information in this presentation is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T). Any opinions contained herein are those of the author and do not necessarily reflect those of DHS S&T. For more information, please contact: Anil John, Program Manager Cybersecurity R&D anil.john@hq.dhs.gov

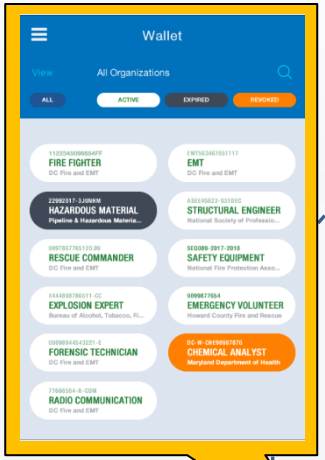
Leverage existing relationships

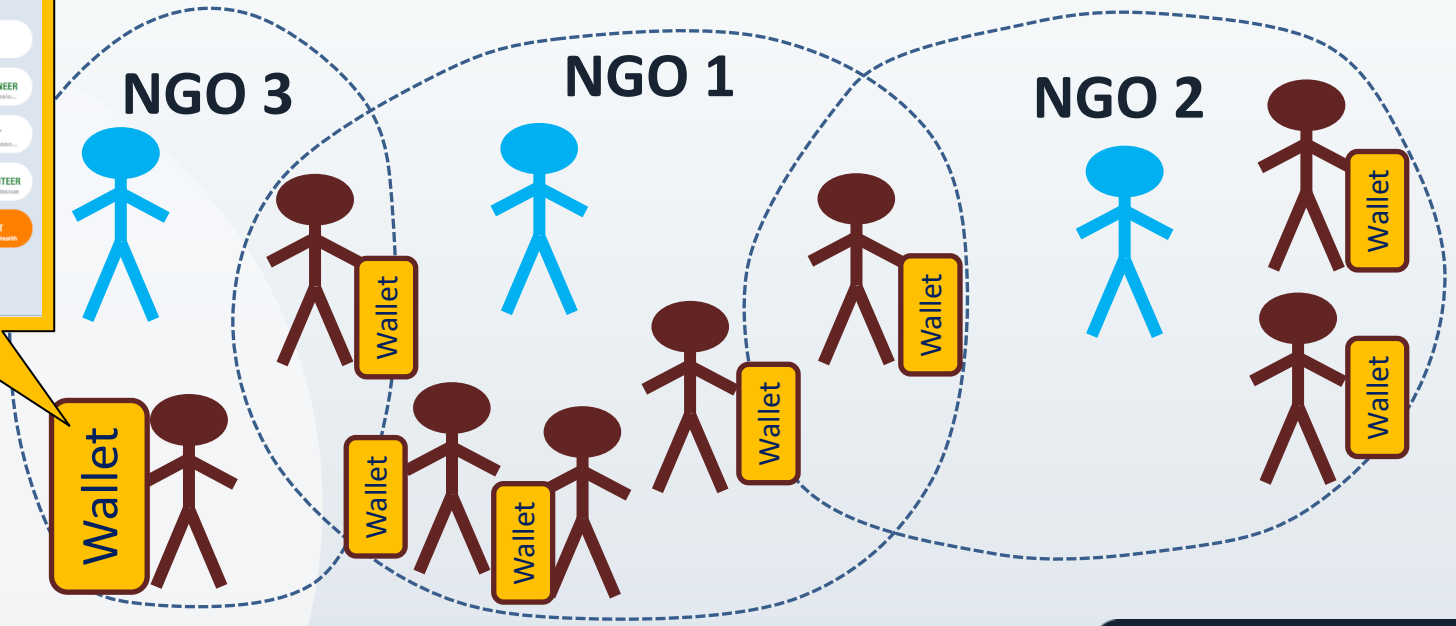
We start with the assumption that vaccine administration today is well enough managed by public health authorities and non-government organisations, and that the records of vaccination kept in the existing paper Yellow Card are fit for purpose. The task of digitising proof of vaccination should preserve existing processes and leverage the relationships field workers have with individuals.



Delegate issuance of digital records (i.e. attributes)

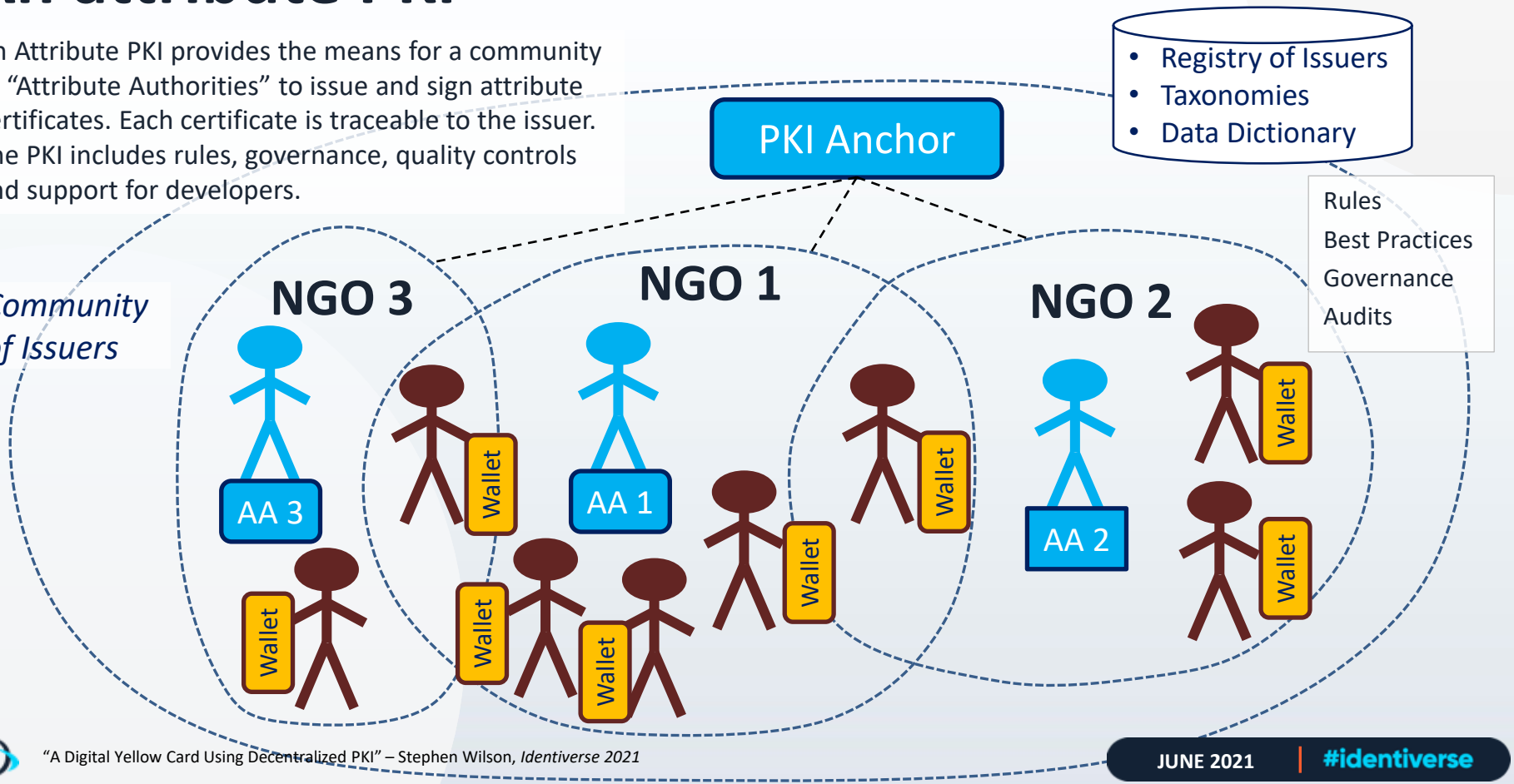
A minimalist solution aims to digitise existing records of vaccination and hold them in a mobile data wallet controlled by each individual. The wallet stores a number of distinct credentials or attributes, each issued by a recognised authority. The MDAV proof of concept represents attributes graphically as *capsules*.





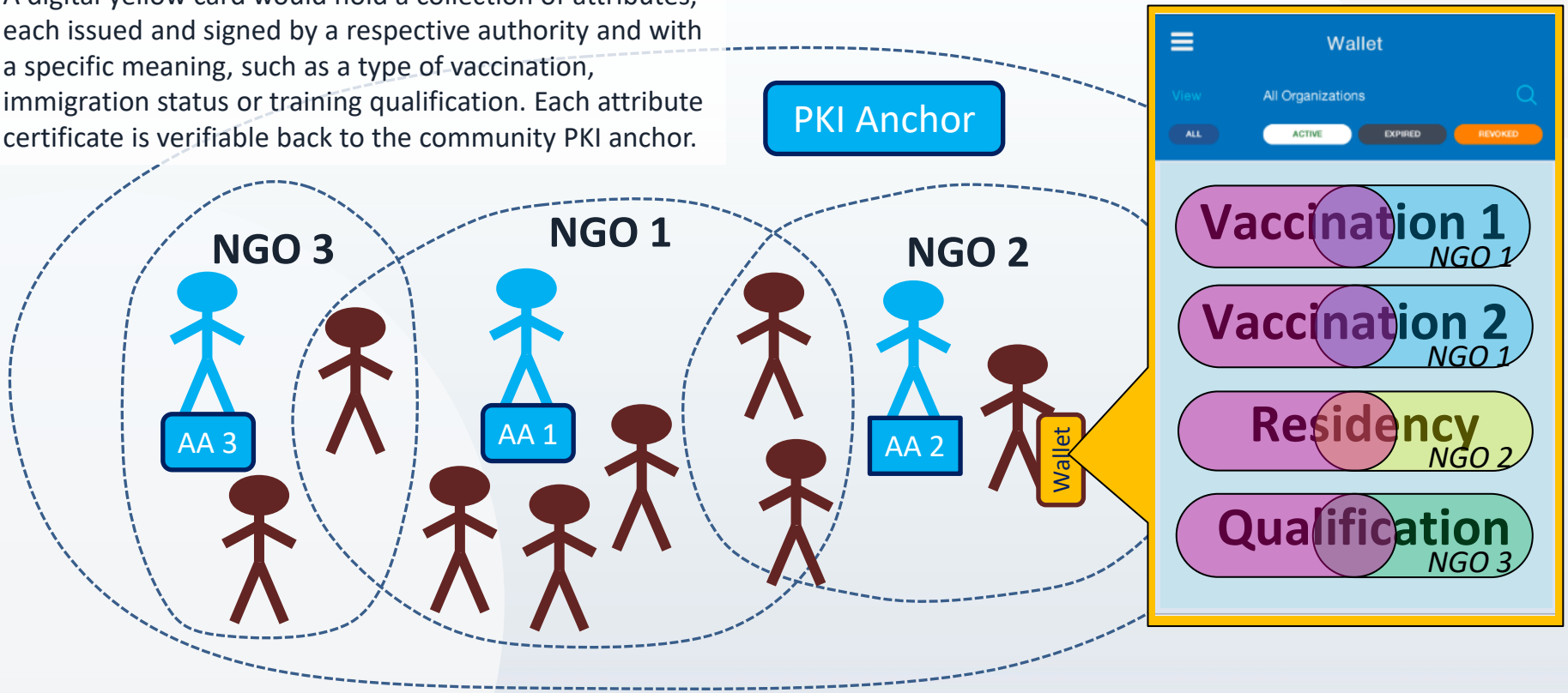
An attribute PKI

An Attribute PKI provides the means for a community of “Attribute Authorities” to issue and sign attribute certificates. Each certificate is traceable to the issuer. The PKI includes rules, governance, quality controls and support for developers.

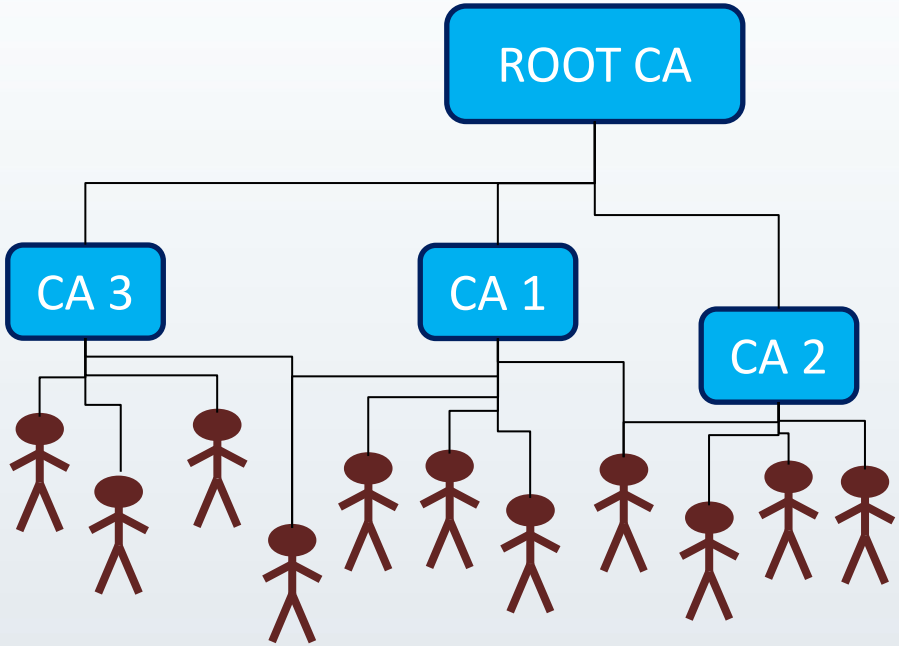


A PKI certificate-based Yellow Card

A digital yellow card would hold a collection of attributes, each issued and signed by a respective authority and with a specific meaning, such as a type of vaccination, immigration status or training qualification. Each attribute certificate is verifiable back to the community PKI anchor.



Compare Traditional PKI …

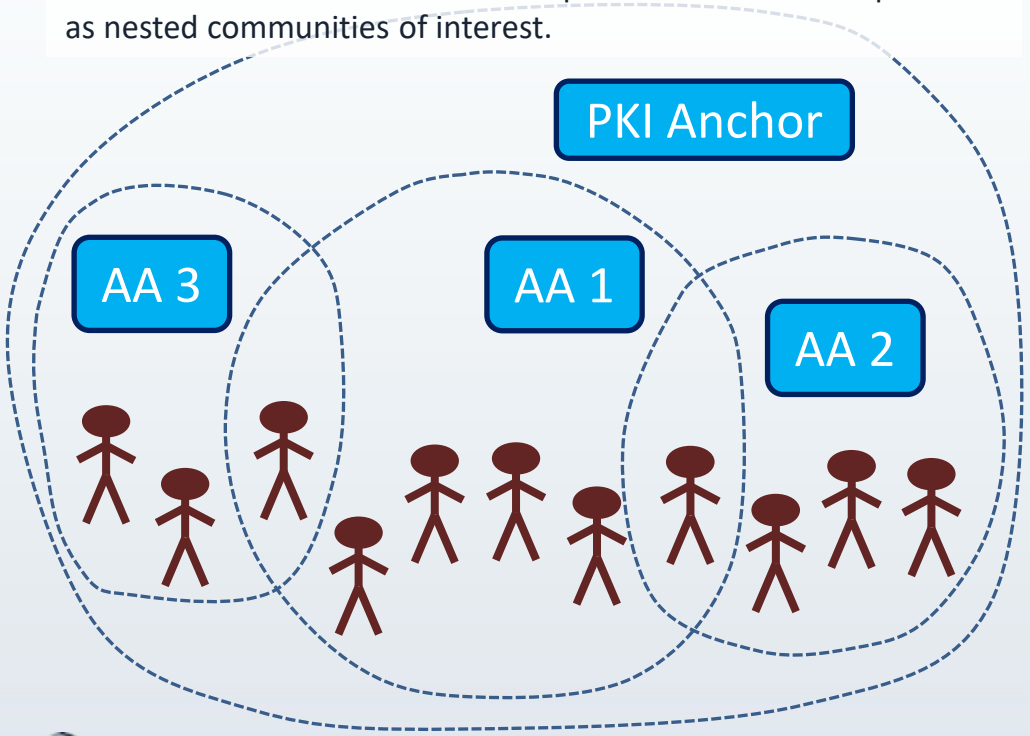


Traditional public key infrastructure was intended for proof-of-identity within rigid governmental applications. Identification policy and issuance rules were set at the top and pushed down from the Root CA. All certificates had the same meaning.

- Hierarchical
- Bureaucratic
- Dictatorial
- Homogenous
- Rigid.

Community PKI

Topologically equivalent to traditional hierarchical PKI – and built from the same X.509-standard components – but re-interpreted as nested communities of interest.



Community PKI does not provide proof-of-identity but rather proof of a particular credential. Issuance rules and policies are set by each sub-community; each certificate has its own meaning, codified in a Certificate Policy. The anchor provide a master key for verifying that each issuer is a bona fide member of the scheme.

- Flexibility
- Accountablity
- Delegation
- Diversity.

Is this an identity issue?

The World Health Organisation has developed interim guidelines for digitised vaccination certificates within the existing Yellow Book framework. Digitisation does not replace the Yellow Book but provides an electronic equivalent. The digital certificate is expressly not a form of identity, and must be issued according to existing healthcare identification processes.

https://www.who.int/publications/m/item/interim-guidance-for-developing-a-smart-vaccination-certificate

- PKI-based global trust network
- Does not supersede Yellow Card
- Certificate *is not an identity*
- Identity shall be established as per Member State norms.

"A Digital Yellow Card Using Decentralized PKI" – Stephen Wilson, *Identiverse 2021*

Conclusions

- PbD: Collection limitation

  No arbitrary identity proofing

- Community PKI preserves relationships

  Tree structured *but not dictatorial*

- No exotic technology

- No identity revolution.