MDAV

Mobile Device Attributes Validation

Cloud Identity Summit
Chicago, 19 June 2017

Steve Wilson
Lockstep Technologies

Acknowledgement

The research in this presentation was conducted under contract with the U.S Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and sponsored by Kantara Initiative Inc.

Any opinions contained herein are those of the author and do not necessarily reflect those of DHS S&T.

MDAV Team Profile

- Lockstep Technologies
  - Steve Wilson (Principal Investigator)
- IDI
  - Adam Madlin (Project Manager)
  - Les Chasen (Development Lead)
- Kantara
  - Ruth Puente, Colin Wallis
- CCICADA, Rutgers University
  - Prof Janne Lindqvist

The need

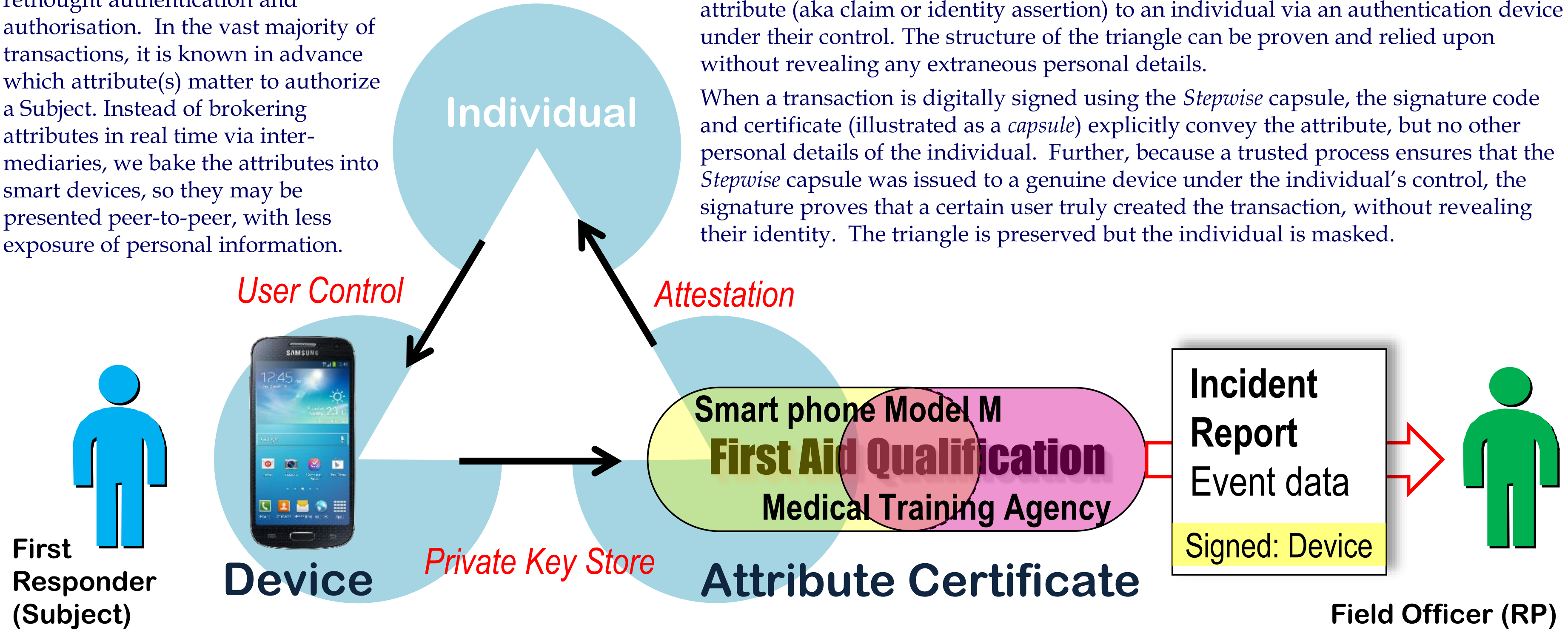
- First Responders (keystone customers)
  - proof of credentials, offline
  - proof of issuer (provenance)
  - tamper resistant storage in mobiles.
- Broader users
  - manage multiple attributes
  - anonymously, pseudonymously
  - decouple attribute issuers, devices, and RPs.

The MDAV Approach

Lockstep has fundamentally rethought authentication and authorisation. In the vast majority of transactions, it is known in advance which attribute(s) matter to authorize a Subject. Instead of brokering attributes in real time via intermediaries, we bake the attributes into smart devices, so they may be presented peer-to-peer, with less exposure of personal information.

Lockstep Technologies' *Stepwise* creates a strong virtual triangle joining a digital attribute (aka claim or identity assertion) to an individual via an authentication device under their control. The structure of the triangle can be proven and relied upon without revealing any extraneous personal details.

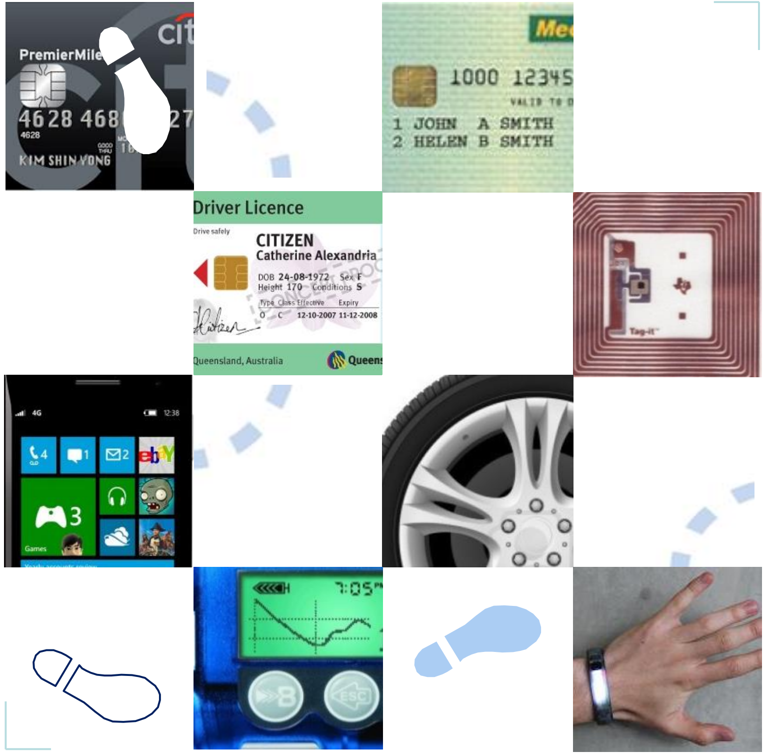
When a transaction is digitally signed using the *Stepwise* capsule, the signature code and certificate (illustrated as a *capsule*) explicitly convey the attribute, but no other personal details of the individual. Further, because a trusted process ensures that the *Stepwise* capsule was issued to a genuine device under the individual's control, the signature proves that a certain user truly created the transaction, without revealing their identity. The triangle is preserved but the individual is masked.



Benefits

- Transforms the integrity and privacy of attributes
- Provenance of attributes, issuers and devices
- Disclosure minimization; anonymous if desired
- Matches many supposed qualities of blockchain yet –
  - works offline
  - fast to process
  - leverages mature, standard PKI stack & services
  - simple, elegant architecture & governance
  - low risk.

Discussion



swilson@lockstep.com.au
http://lockstep.com.au