PKI post Blockchain

Cloud Identity Summit
Chicago, 20 June 2017

Steve Wilson
Lockstep Technologies

Acknowledgement

Certain 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.

A mood for change

We're in the mood for change. Decentralisation and self-determination are on the minds of many, given the power imbalances in the digital economy. The anti-establishment blockchain came along at just the right time! It promises (apparently) to totally empower individuals. Openness and disintermediation are among the rallying calls of the Self Sovereign identity movement, where blockchain has attached itself.

Meanwhile, orthodox Federated Identity has always been easier said than done. There is still no successful market-driven cross-sector federation, despite umpteen frameworks and public-private pilots in the US, the UK, Australia and elsewhere.

An underlying weakness is we still tend to treat identity as one-dimensional. Identity management practices perpetuate simplistic 'Good / Better / Best' Levels of Assurance. We act like identity is "all we got"; we habitually deal with increased risk by simply piling on more identification.


“Hello, Identity Service?
Send up more identity!”

But ever since CIS 2013 there has been an Attributes Push. A great many analyses and initiatives all shift the focus from general purpose identity down to special purpose attributes. See for example Confyrm's work on signals, the FIDO Alliance (which disavows identification and only solves for authentication), Vectors of Trust, W3C Verified Claims, Sovrin, and SecureKey. Today we will look at the latest, Lockstep's MDAV project in the Kantara Identity and Privacy Incubator, funded by DHS Science & Technology.

Authentication

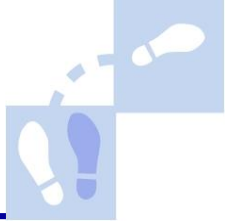
The means by which a receiver of an electronic transaction or message makes a decision to accept or reject that transaction or message.

APEC eSecurity Task Group 1997

Attributes supply chains

	Why?	What?	How?
Design Time	**Define Attribute(s)**	`Customer Ref No.`	Service Provider
		`Account No.`	Institution
		`Age`	Govt / Other Broker
		`Qualification`	Credentialing Body
		`Qualification ...`	Credentialing Body ...
Enrolment Time	**Prove & Save Attributes**		Signed by authority, ***and*** Saved to a device, ***or*** Saved to a ledger, ***or*** Left with the authority …
Transaction Time	*There have always be numerous sources of truth about the people and entities we want to deal with – their qualifications, memberships, affiliations, vital statistics, reputations and so on. Generally referred to as "attributes", these data are available through digital supply chains. The attributes of interest can be defined in advance of most transactions, and registered and stored in a number of ways. There is a great contest of ideas in identity management as to how these attributes should be conveyed.*		**Obtain & Check Attribute(s)**

Case study: MDAV



A simple re-configuration of standard public key certificates allows them to convey concrete attributes, one by one, for 'atomic' authentication or authorization use cases (as opposed to the classic formulation of singular general purpose identity certificates). These new forms of attribute certificates share some of the attractive qualities of blockchain, so we present them here as "Post Blockchain PKI".

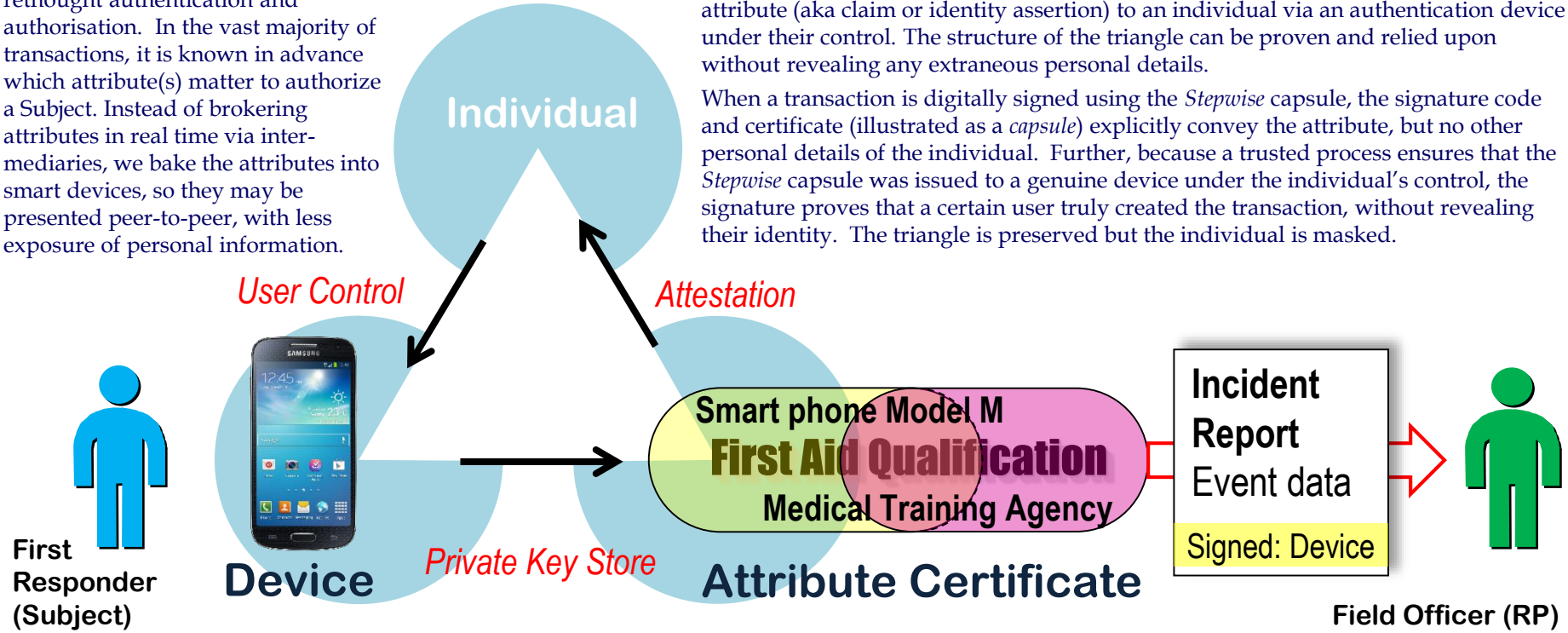
- ***Mobile Device Attributes Validation***
- **Kantara Identity & Privacy Incubator KIPI**
- **Reprise *Attribute Certificates!***
- **First Responder use case**
- **Extensible to KYC, Personal Data Stores …**

The MDAV Approach

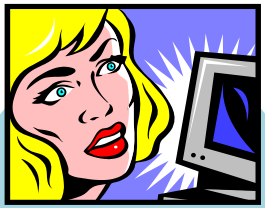
Lockstep has fundamentally rethought authentication and authorisation. In the vast majority of transactions, it is known in advance which attribute(s) matter to authorize a Subject. Instead of brokering attributes in real time via inter-mediaries, we bake the attributes into smart devices, so they may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

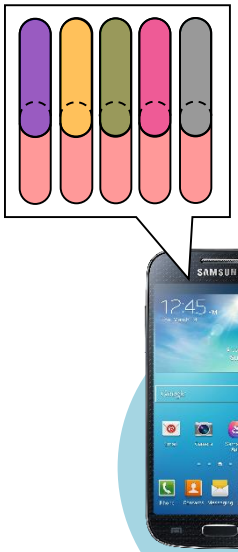
Lockstep Technologies' *Stepwise* creates a strong virtual triangle joining a digital attribute (aka claim or identity assertion) to an individual via an authentication device under their control. The structure of the triangle can be proven and relied upon without revealing any extraneous personal details.

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.



General use case: KYC and PDS





Smart phone Model M
Driver Lic. 123456
State DMV
→ Bank

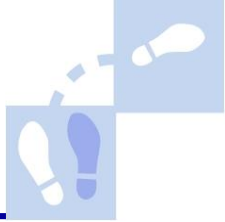
Smart phone Model M
DOB 1 Jan 1980
Register of Births
→ Bank

Smart phone Model M
101 First Ave Small Town
Post Office
→ Bank

Smart phone Model M
Age > 21
Bank One
→ Gaming

The attribute certificate approach being piloted with the DHS MDAV project can be extended to Personal Data Stores (PDSes) for use cases like proving the provenance of personal details under Know Your Customer rules.

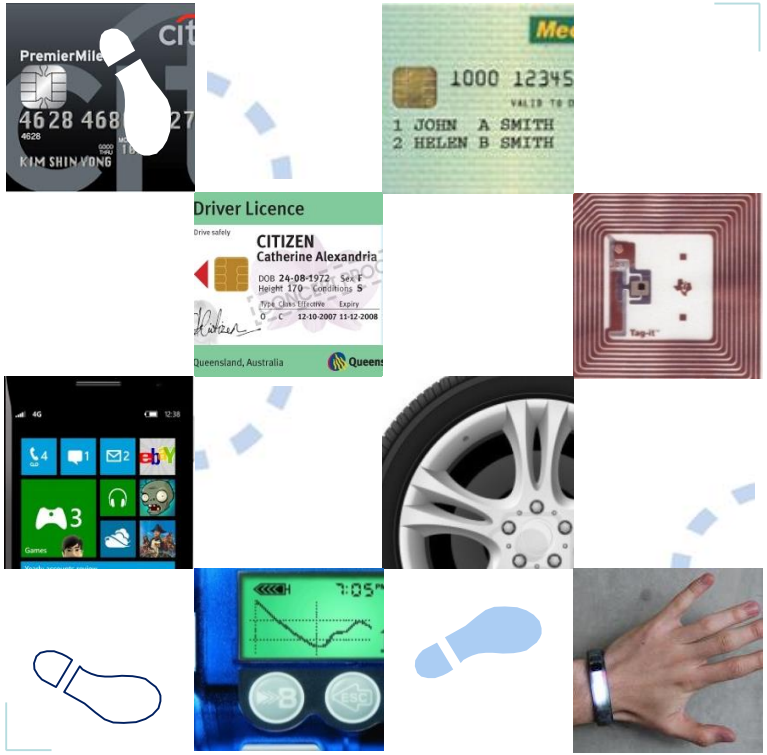
PKI redux



The MDAV approach of baking attribute values into attribute certificates turns out to mirror several popular qualities of blockchain or distributed ledger technologies, but uses a far more mature and lower risk technology stack. With the contest of ideas around attributes, provenance and decentralised ledgers, MDAV shows how there is life and innovation yet in PKI.

- **Decentralised, peer-to-peer presentation**
- **Works with contestable attribute sources**
- **Minimises disclosure of PII**
- **Mature technology**
- **Standards-based.**

Discussion



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