Mobile Device Attributes Validation – MDAV

International Identity Summit
University of Washington
6-7 September 2018

Steve Wilson
ValidIDy

Acknowledgement

Information in this presentation and/or video is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T).

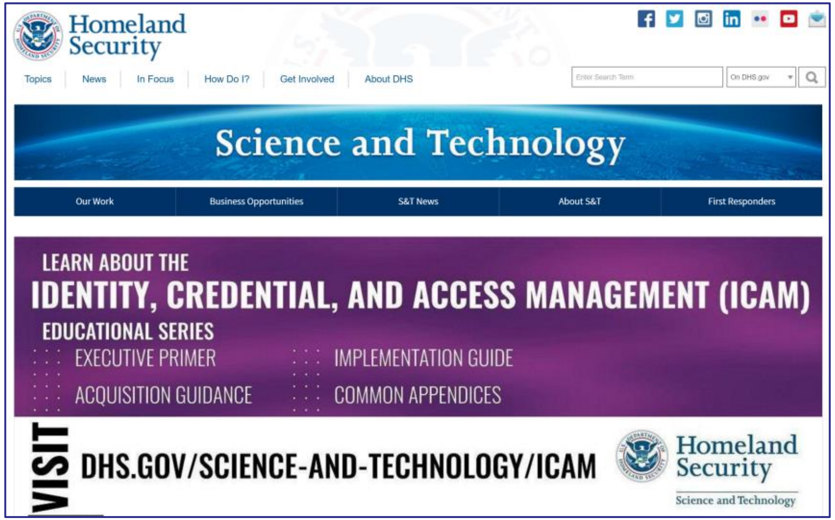
Any opinions contained herein are those of the performer and do not necessarily reflect those of DHS S&T.

For more information, please contact
Anil John, Program Manager Cybersecurity R&D
anil.john@hq.dhs.gov

Announcement

Lockstep Technologies, an Australian research & development company, has been contracted by DHS S&T through a three phase project to prove the MDAV solution and mature it towards commercial reality. While Lockstep's contract with DHS is continuing through Phase 3, we are launching a new operation to take the solution to market. That business is called ValidIDy. It was announced at the International Identity Summit on September 7.

DHS Science & Technology



Homeland Security

Topics | News | In Focus | How Do I? | Get Involved | About DHS

Enter Search Term | On DHS.gov

Science and Technology

Our Work | Business Opportunities | S&T News | About S&T | First Responders

LEARN ABOUT THE

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

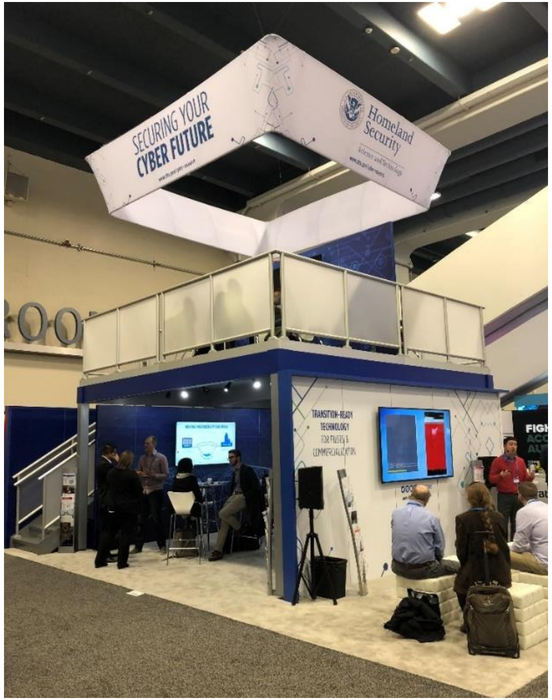
EDUCATIONAL SERIES

- EXECUTIVE PRIMER
- IMPLEMENTATION GUIDE
- ACQUISITION GUIDANCE
- COMMON APPENDICES

VISIT DHS.GOV/SCIENCE-AND-TECHNOLOGY/ICAM

Homeland Security

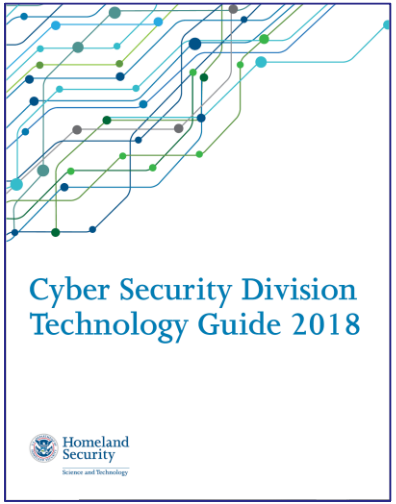
Science and Technology



We acknowledge the outreach performed by DHS S&T, such as its conference activities, and the support it provides to its performers and the security R&D community.

DHS Science & Technology

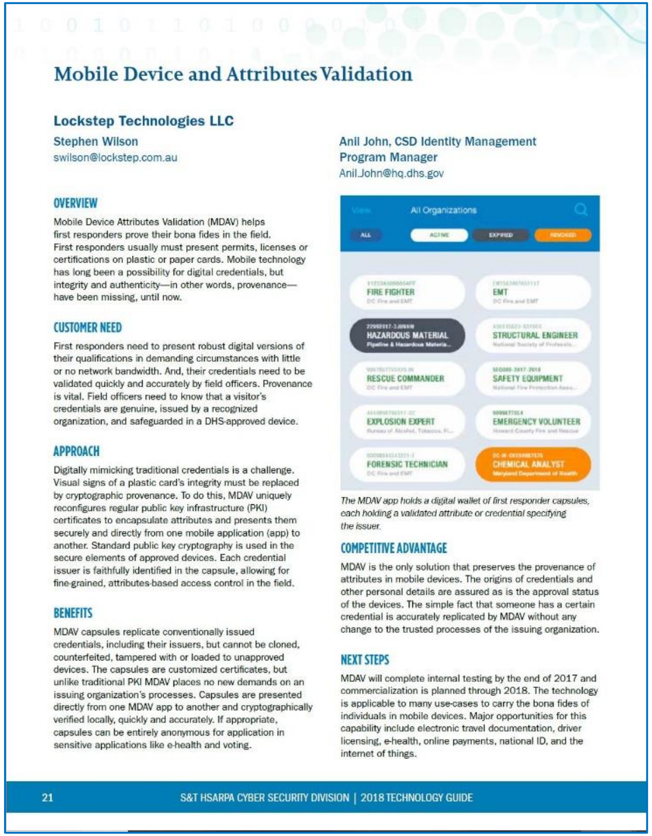
*DHS produces an annual compendium of its research programs and partners. See **https://www.dhs.gov/sites/default/files/publications/CSD%202018%20Tech_Guide_Web%20Version_508.pdf** (PDF).*



Cyber Security Division Technology Guide 2018

Homeland Security
Science and Technology

The Cyber Security Division publishes an annual guide, with details of its "performer" projects, including Lockstep Technologies' MDAV.



Mobile Device and Attributes Validation

Lockstep Technologies LLC
Stephen Wilson
swilson@lockstep.com.au

Anil John, CSD Identity Management Program Manager
Anil.John@hq.dhs.gov

OVERVIEW

Mobile Device Attributes Validation (MDAV) helps first responders prove their bona fides in the field. First responders usually must present permits, licenses or certifications on plastic or paper cards. Mobile technology has long been a possibility for digital credentials, but integrity and authenticity—in other words, provenance—have been missing, until now.

CUSTOMER NEED

First responders need to present robust digital versions of their qualifications in demanding circumstances with little or no network bandwidth. And, their credentials need to be validated quickly and accurately by field officers. Provenance is vital. Field officers need to know that a visitor's credentials are genuine, issued by a recognized organization, and safeguarded in a DHS-approved device.

APPROACH

Digitally mimicking traditional credentials is a challenge. Visual signs of a plastic card's integrity must be replaced by cryptographic provenance. To do this, MDAV uniquely reconfigures regular public key infrastructure (PKI) certificates to encapsulate attributes and presents them securely and directly from one mobile application (app) to another. Standard public key cryptography is used in the secure elements of approved devices. Each credential issuer is faithfully identified in the capsule, allowing for fine-grained, attributes-based access control in the field.

BENEFITS

MDAV capsules replicate conventionally issued credentials, including their issuers, but cannot be cloned, counterfeited, tampered with or loaded to unapproved devices. The capsules are customized certificates, but unlike traditional PKI MDAV places no new demands on an issuing organization's processes. Capsules are presented directly from one MDAV app to another and cryptographically verified locally, quickly and accurately. If appropriate, capsules can be entirely anonymous for application in sensitive applications like e-health and voting.

The MDAV app holds a digital wallet of first responder capsules, each holding a validated attribute or credential specifying the issuer.

COMPETITIVE ADVANTAGE

MDAV is the only solution that preserves the provenance of attributes in mobile devices. The origins of credentials and other personal details are assured as is the approval status of the devices. The simple fact that someone has a certain credential is accurately replicated by MDAV without any change to the trusted processes of the issuing organization.

NEXT STEPS

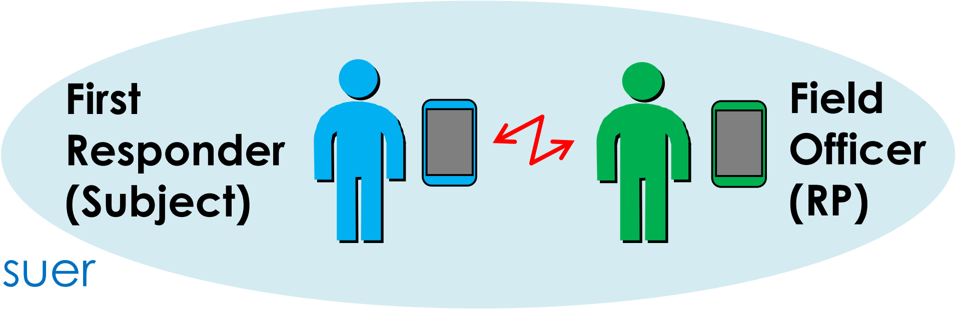
MDAV will complete internal testing by the end of 2017 and commercialization is planned through 2018. The technology is applicable to many use-cases to carry the bona fides of individuals in mobile devices. Major opportunities for this capability include electronic travel documentation, driver licensing, e-health, online payments, national ID, and the internet of things.

21 S&T HSARPA CYBER SECURITY DIVISION | 2018 TECHNOLOGY GUIDE

MDAV Team Profile

- Lockstep Technologies / ValidIDy
  - Adam Madlin – Project Manager & Business Development
  - Les Chasen – Architect and Technical Lead
  - Steve Wilson – Managing Director
  - Bruce Goldsmith – Business Development.
- Kantara Identity & Privacy Incubator (KIPI)
  - Ruth Puente, Colin Wallis.
- CCICADA, Rutgers University
  - Prof Janne Lindqvist.

The need

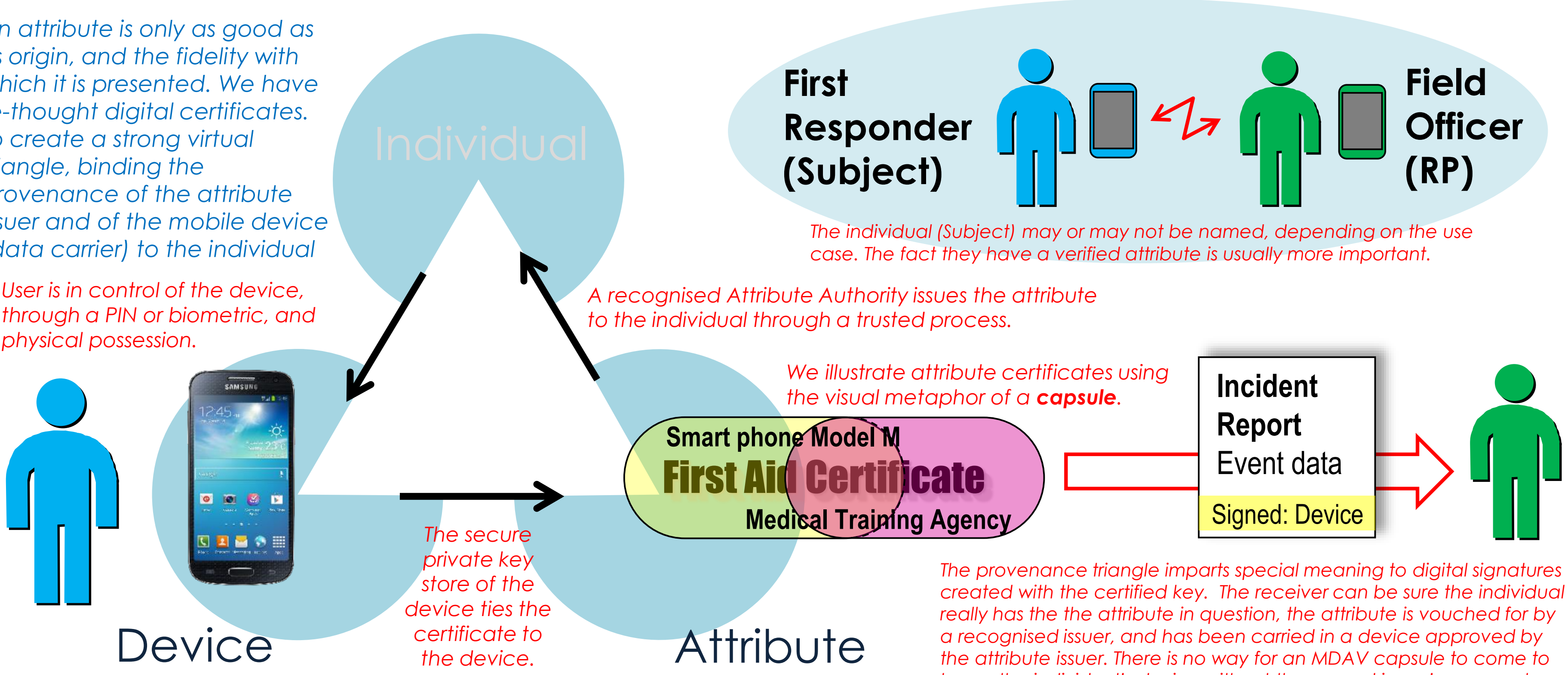


- First Responders
  - mobile credentials essential
  - must prove *provenance* of issuer
  - and provenance of the device as trusted data carrier
  - in challenging low/zero network settings.
- Broader users
  - many use cases need to manage multiple identity attributes
  - sometimes anonymously or pseudonymously
  - security functions span access control and document authorization.

Attribute Certificates

An attribute is only as good as its origin, and the fidelity with which it is presented. We have re-thought digital certificates. to create a strong virtual triangle, binding the provenance of the attribute issuer and of the mobile device (data carrier) to the individual

User is in control of the device, through a PIN or biometric, and physical possession.



The individual (Subject) may or may not be named, depending on the use case. The fact they have a verified attribute is usually more important.

A recognised Attribute Authority issues the attribute to the individual through a trusted process.

*We illustrate attribute certificates using the visual metaphor of a **capsule**.*

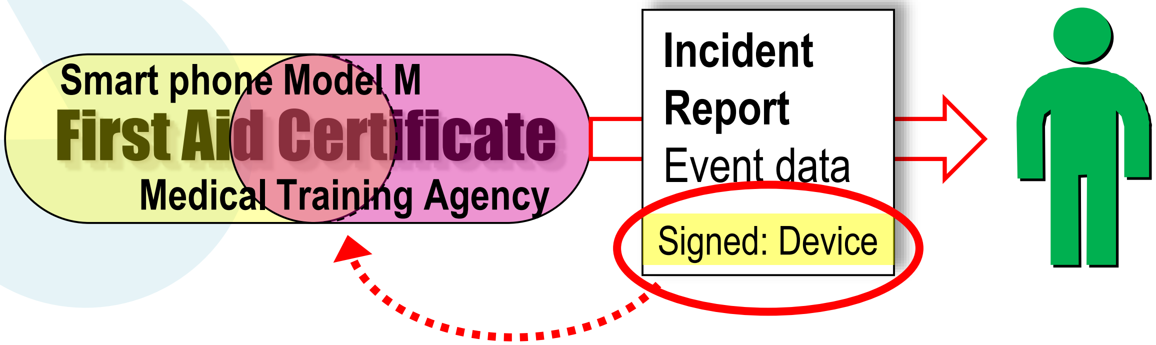
The secure private key store of the device ties the certificate to the device.

The provenance triangle imparts special meaning to digital signatures created with the certified key. The receiver can be sure the individual really has the the attribute in question, the attribute is vouched for by a recognised issuer, and has been carried in a device approved by the attribute issuer. There is no way for an MDAV capsule to come to be on the individual's device without the named issuer's approval.

Attribute Certificates

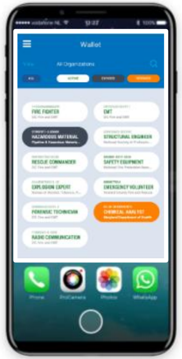
Verifying a digital signature against a capsule proves:

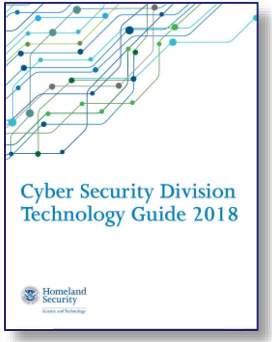
- the attribute is true, according to the named issuing authority
- the attribute owner was in control when it was presented
- the attribute carrier is genuine and approved by the authority.



MDAV *Execution* – complete

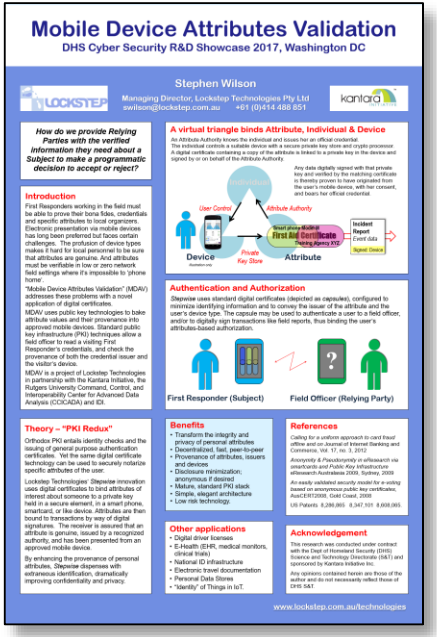
- Deliverables of the *Execution* phase
  - Working & tested prototype in the App Store
  - Architecture (available on request)
  - Video and Marketing Brief (public)
- Presented at the Cloud Identity Summit, Chicago, June 2017
- Cyber Showcase, Washington, July 2017
- Featured in DHS Science & Technology Cyber Security Technology Guide 2018.





Cyber Security Division
Technology Guide 2018

Homeland Security
Science and Technology



Mobile Device Attributes Validation

DHS Cyber Security R&D Showcase 2017, Washington DC

Stephen Wilson
Managing Director, Lockstep Technologies Pty Ltd
swilson@lockstep.com.au +61 (0)414 488 851

How do we provide Relying Parties with the verified information they need about a Subject to make a programmatic decision to accept or reject?

Introduction

First Responders working in the field must be able to prove their bona fides, credentials and specific attributes to local organizers. Electronic presentation via mobile devices has long been preferred but faces certain challenges. The profusion of device types makes it hard for local personnel to be sure that attributes are genuine. And attributes must be verifiable in low or zero network field settings where it's impossible to 'phone home'.

"Mobile Device Attributes Validation" (MDAV) addresses these problems with a novel application of digital certificates.

MDAV uses public key technologies to bake attribute values and their provenance into approved mobile devices. Standard public key infrastructure (PKI) techniques allow a field officer to read a visiting First Responder's credentials, and check the provenance of both the credential issuer and the visitor's device.

MDAV is a project of Lockstep Technologies in partnership with the Kantara Initiative, the Rutgers University Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA) and IDI.

A virtual triangle binds Attribute, Individual & Device

An Attribute Authority knows the individual and issues her an official credential.
The individual controls a suitable device with a secure private key store and crypto processor.
A digital certificate containing a copy of the attribute is linked to a private key in the device and signed by or on behalf of the Attribute Authority.

Any data digitally signed with that private key and verified by the matching certificate is thereby proven to have originated from the user's mobile device, with her consent, and bears her official credential.

Authentication and Authorization

Stepwise uses standard digital certificates (depicted as *capsules*), configured to minimize identifying information and to convey the issuer of the attribute and the user's device type. The capsule may be used to authenticate a user to a field officer, and/or to digitally sign transactions like field reports, thus binding the user's attributes-based authorization.

Theory – "PKI Redux"

Orthodox PKI entails identity checks and the issuing of general purpose authentication certificates. Yet the same digital certificate technology can be used to securely notarize specific attributes of the user.

Lockstep Technologies' *Stepwise* innovation uses digital certificates to bind attributes of interest about someone to a private key held in a secure element, in a smart phone, smartcard, or like device. Attributes are then bound to transactions by way of digital signatures. The receiver is assured that an attribute is genuine, issued by a recognized authority, and has been presented from an approved mobile device.

By enhancing the provenance of personal attributes, *Stepwise* dispenses with extraneous identification, dramatically improving confidentiality and privacy.

Benefits

- Transform the integrity and privacy of personal attributes
- Decentralized, fast, peer-to-peer
- Provenance of attributes, issuers and devices
- Disclosure minimization; anonymous if desired
- Mature, standard PKI stack
- Simple, elegant architecture
- Low risk technology.

Other applications

- Digital driver licenses
- E-Health (EHR, medical monitors, clinical trials)
- National ID infrastructure
- Electronic travel documentation
- Personal Data Stores
- "Identity" of Things in IoT.

References

Calling for a uniform approach to card fraud offline and on Journal of Internet Banking and Commerce, Vol. 17, no. 3, 2012

Anonymity & Pseudonymity in eResearch via smartcards and Public Key Infrastructure eResearch Australasia 2009, Sydney, 2009

An easily validated security model for e-voting based on anonymous public key certificates, AusCERT2008, Gold Coast, 2008

US Patents 8,286,865 8,347,101 8,608,065.

Acknowledgement

This research was conducted under contract with the Dept 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.

www.lockstep.com.au/technologies

MDAV *Transition phase*

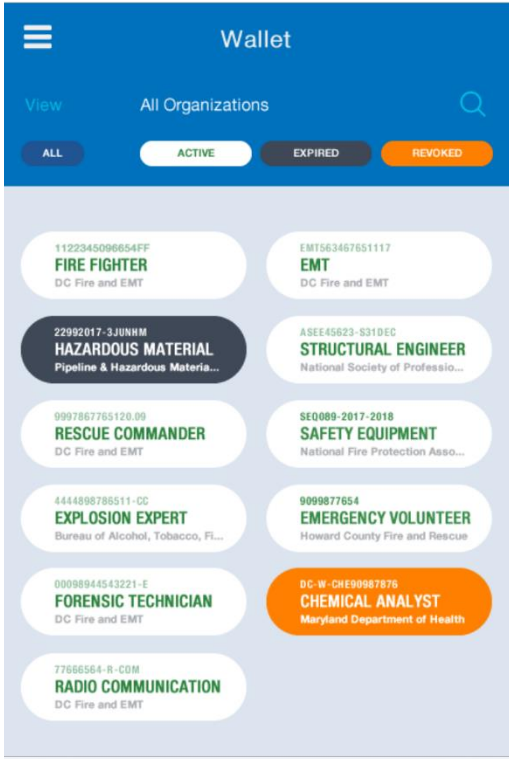
1. Core infrastructure build
2. Developer integration (APIs, policy templates)
3. Proof-of-Concept candidates:
   - Financial Services (“KYC Once”, Card Not Present payments)
   - Clinical trials investigator and/or patient anonymization
   - Personal Data Wallet

- Launch **ValidIDy** http://valididy.com

MDAV Benefits

- Transforms the integrity & privacy of personal attributes
- *Provenance* of attributes, issuers *and* data carriers
- 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 technology risk; low project risk.

Conclusion



1122345096654FF
FIRE FIGHTER
DC Fire and EMT

EMT563467651117
EMT
DC Fire and EMT

22992017-3JUNHM
HAZARDOUS MATERIAL
Pipeline & Hazardous Materia...

ASEE45623-S31DEC
STRUCTURAL ENGINEER
National Society of Professio...

9997867765120.09
RESCUE COMMANDER
DC Fire and EMT

SEQ089-2017-2018
SAFETY EQUIPMENT
National Fire Protection Asso...

4444898786511-CC
EXPLOSION EXPERT
Bureau of Alcohol, Tobacco, Fi...

9099877654
EMERGENCY VOLUNTEER
Howard County Fire and Rescue

00098944543221-E
FORENSIC TECHNICIAN
DC Fire and EMT

DC-W-CHE90987876
CHEMICAL ANALYST
Maryland Department of Health

77666564-R-COM
RADIO COMMUNICATION
DC Fire and EMT

It an attribute of an individual is known to be true 'in real life', thanks to the authority of its trusted issuer, then ValidIDy proves it's also true online.

privacy
security
truth

steve.wilson@valididy.com
http://valididy.com