Mobile Device Attributes Validation – MDAV

International Identity Summit
University of Washington
6-7 August 2018

Steve Wilson
ValidIDy

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).

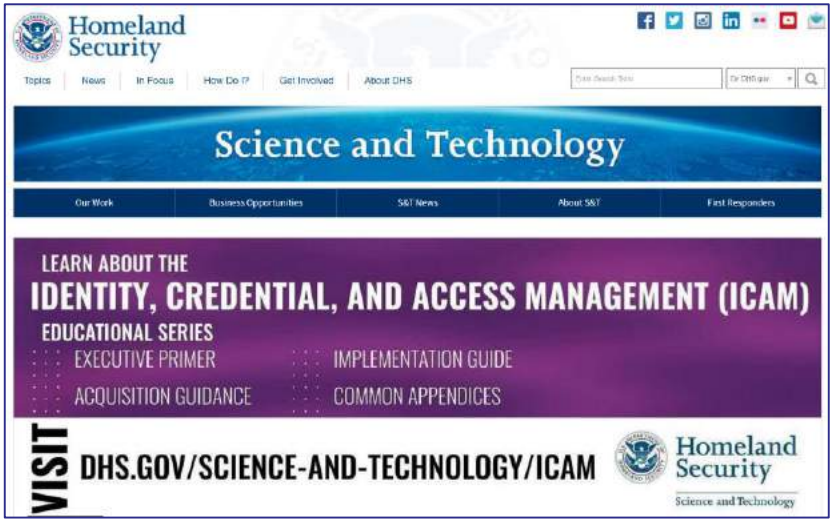
Any opinions contained herein are those of the performer and do not necessarily reflect those of DHS S&T.

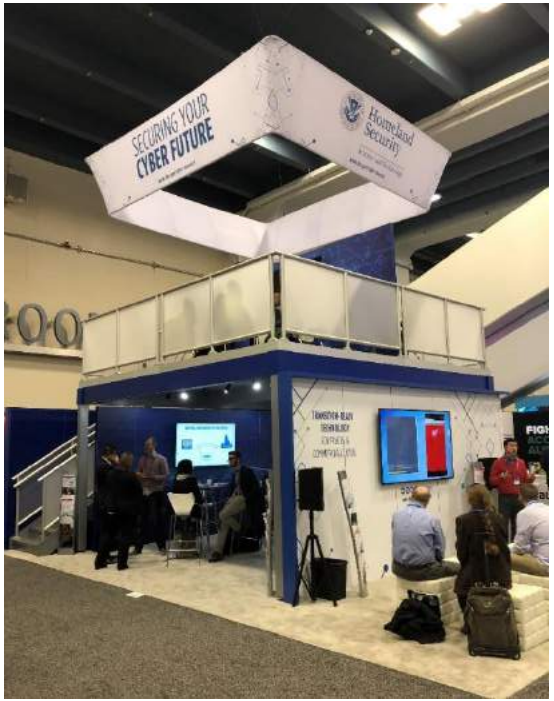
For more information, please contact
Anil John, Program Manager Cybersecurity R&D
anil.john@hq.dhs.gov

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

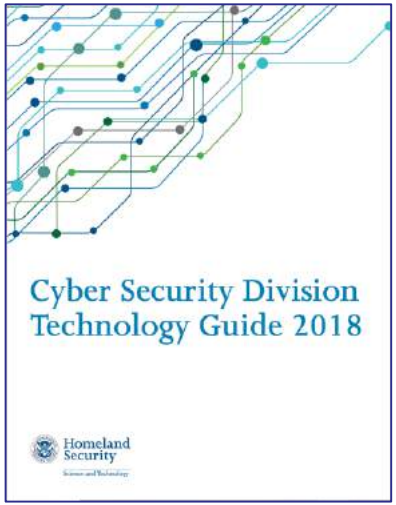




We acknowledge the outreach performed by DHS S&T, such as its conference activities, and the support it provides to its performers and the security R&D community.

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).*



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.

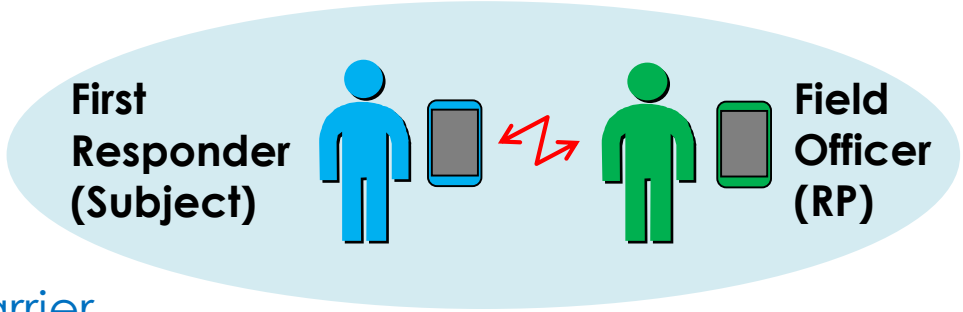
NEXT STEPS

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.

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.

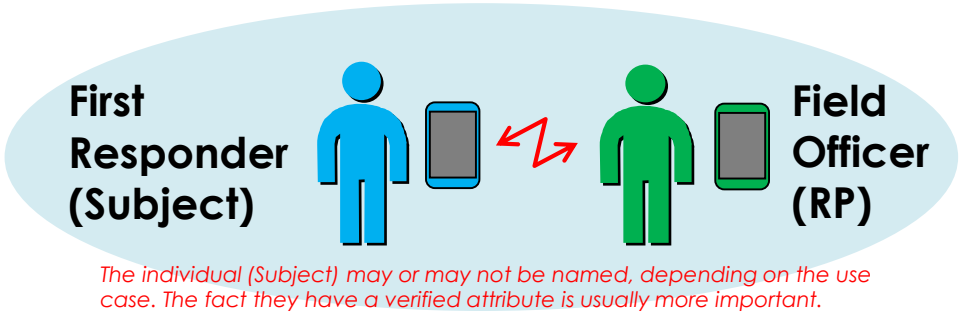
The need



- First Responders
  - mobile credentials
  - Need provenance of issuer
  - And provenance of data carrier
  - In challenging low/zero network settings.
- Broader users
  - Many use cases need to manage multiple identity attributes
  - Sometimes anonymously or pseudonymously
  - Security spans 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 both the attribute issuer and the data carrier to the individual.



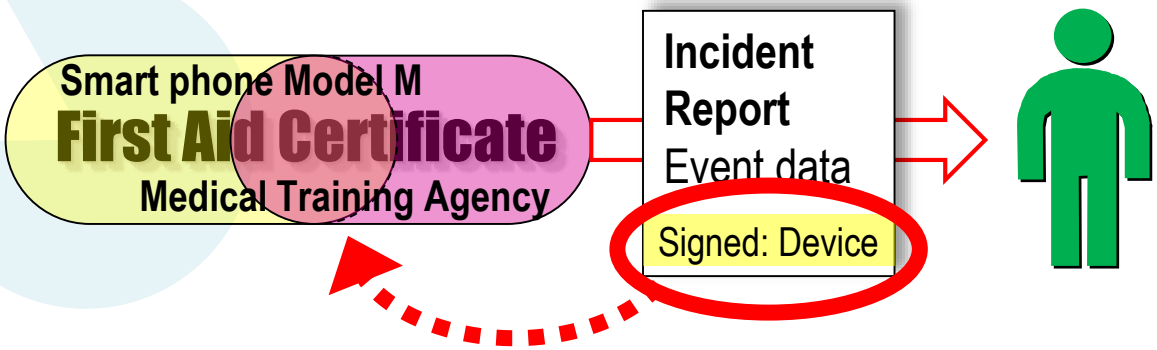
The individual (Subject) may or may not be named, depending on the use case. The fact they have a verified attribute is usually more important.

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, it came from a recognised issuer, and was carried in a device approved by the attribute issuer. There is no way for an MDAV certificate (attribute capsule) to come to be on the individual's phone without the issuer's authority.

Attribute Certificates

Verifying a digital signature against a capsule proves:

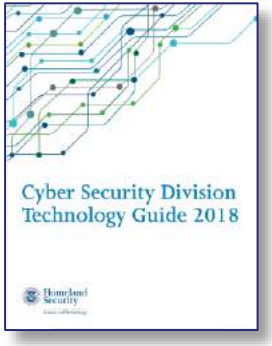
- The attribute is true, according to the named issuing authority
- the attribute owner was in control when it was presented
- The attribute carrier was genuine and approved by the authority.



MDAV Phase 2 *Execution*

- Deliverables
  - Working & Tested Prototype
  - Architecture (available on request)
  - Video and Marketing Brief (public)

- Cloud Identity Summit, Chicago, June 2017
- Cyber Showcase, Washington July 2017
- DHS Science & Technology Cyber Security Technology Guide 2018.



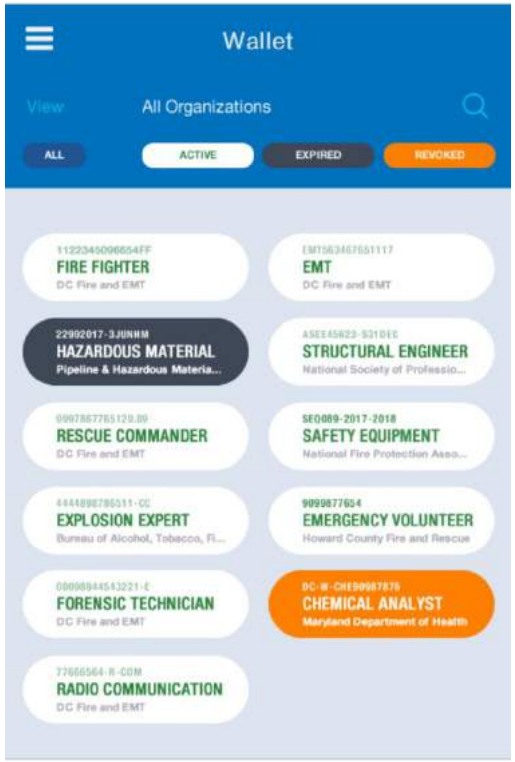
MDAV Phase 3 *Transition*

- Core infrastructure build
- Developer integration (APIs, policy templates)
- Proofs of Concept
  - 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 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 technology risk; low project risk.

Conclusion



It a critical attribute of an individual is known to be true 'in real life', thanks to the authority of its trusted issuer, then we show that it's still true in digital form.

privacy
security
truth

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

VALIDIDY