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.

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.

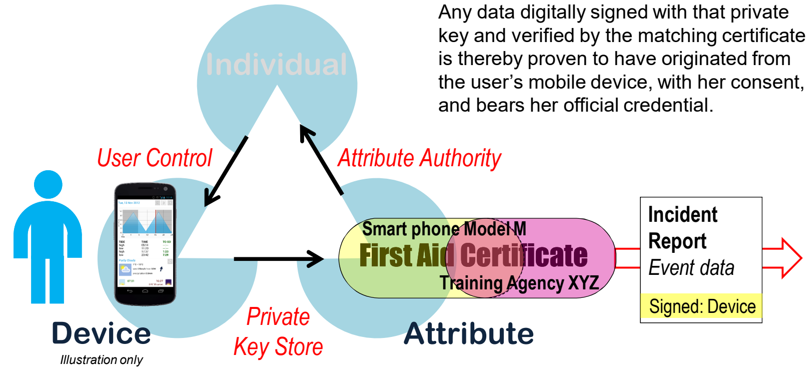
Lockstep Technologies' *Stepwise* innovation uses digital certificates to bind attributes of interest about someone to a private key held in a secure element, in a smart phone, smartcard, or like device. Attributes are then bound to transactions by way of digital signatures. The receiver is assured that 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.

A virtual triangle binds Attribute, Individual & Device

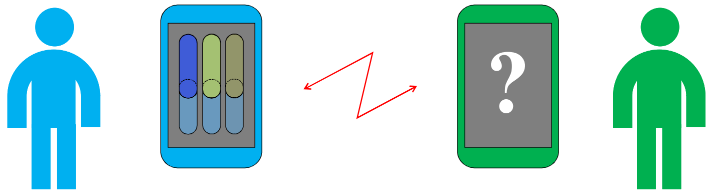
An Attribute Authority knows the individual and issues her an official credential.
The individual controls a suitable device with a secure private key store and crypto processor.
A digital certificate containing a copy of the attribute is linked to a private key in the device and signed by or on behalf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



First Responder (Subject) Field Officer (Relying Party)

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