

# Mobile Device Attribute Validation

## Technology Demonstration Report

June 2019



**Homeland  
Security**

Science and Technology





---

The *Mobile Device Attribute Validation Technology Demonstration Report* was prepared by the National Urban Security Technology Laboratory, U.S. Department of Homeland Security, Science and Technology Directorate.

The views and opinions of authors expressed herein do not necessarily reflect those of the U.S. government.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. government.

With respect to documentation contained herein, neither the U.S. government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the U.S. government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed; nor do they represent that its use would not infringe privately owned rights.

The images included herein were provided by Lockstep Technologies, unless otherwise noted.

---



## FOREWORD

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) contributes to enhancing the security and resilience of the nation's critical information infrastructure and the internet. S&T accomplishes this mission by:

- Developing and delivering new technologies, tools and techniques to enable DHS and the United States to defend, mitigate and secure current and future systems, networks and infrastructure against cyberattacks
- Conducting and supporting technology transition
- Leading and coordinating research and development (R&D) among the R&D community, which includes department customers, government agencies, the private sector and international partners.

To this end, S&T works with an industry partner to develop a mobile application (app) that authenticates first responders' credentials. The app—which uses X.509 public key cryptography on smartphones—aims to enable first responders to verify one another's credentials, permits and certifications quickly, securely and privately during field operations, even when there is no network connectivity.

DHS S&T requested that National Urban Security Technology Laboratory (NUSTL) conduct a technology demonstration to share with first responders the app's capabilities and operational suitability, and to verify and document that the project goals were achieved.

NUSTL reports are posted on the First Responder Communities of Practice (FRCoP) website, a professional networking, collaboration and communication platform created by the DHS S&T to support improved collaboration and information sharing amongst the nation's first responders. This vetted community of members focuses on emergency preparedness, response, recovery and other homeland security issues. To request an FRCoP account, complete an online form at the [first responder website](#).



## POINTS OF CONTACT

National Urban Security Technology Laboratory  
U.S. Department of Homeland Security  
Science and Technology Directorate  
201 Varick Street  
New York, NY 10014

E-mail: [NUSTL@hq.dhs.gov](mailto:NUSTL@hq.dhs.gov)

Website: [www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory](http://www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory)

Authors:

Blaise Linn, Tech Demo Test Director, Systems Engineering Technical Assistance Support Contractor  
Tyler Mackanin, Systems Engineering Technical Assistance Support Contractor

---



## EXECUTIVE SUMMARY

Lockstep Technologies is developing the Mobile Device Attribute Validation (MDAV) application for the U.S. Department of Homeland Security (DHS), Science and Technology Directorate (S&T). MDAV is a mobile application that digitally authenticates first responders' credentials. Using X.509 public key cryptography on smartphones, the MDAV app aims to enable first responders to verify one another's credentials, permits and certifications quickly, securely and privately during field operations, even when there is no network connectivity.

MDAV has two main mobile components: a wallet that contains the responder's credentials in a cryptographically secure form, and a reader that scans and validates those credentials. Credentials are relayed between phones via several methods (such as Quick Response Codes, Near Field Communication and Bluetooth), and verified electronically. Additionally, there is a web application used by administrators (attribute authorities) to issue the credentials.

On December 11, 2018, the National Urban Security Technology Laboratory conducted a technology demonstration (tech demo) of MDAV with Lockstep Technologies. The purpose of the tech demo was to assist DHS S&T and its contracted developer, Lockstep Technologies, in gathering feedback from emergency response personnel on the concept and design of the MDAV application. During the tech demo, evaluators from the New York City Police Department and New York City Emergency Management (NYCEM) observed demonstrations of MDAV's functionality, used the app and provided feedback.

NYCEM was interested in the technology and described additional features that would make it more suitable for their use, such as adding the ability to transfer credentials from multiple responders simultaneously to the incident commander, the ability to send multiple certifications at a time from each responder to the incident commander and the ability to view a list of responders with a particular skill at a scene. Overall, evaluators agreed that MDAV would be useful during large-scale responses that require mutual aid agreements to be activated, but it is unlikely to be needed for day-to-day operations as there is no need to verify credentials of outside agencies during typical operations.



## TABLE OF CONTENTS

1.0 Introduction.....	8
1.1 Purpose .....	10
1.2 Objective .....	10
1.3 Requirements .....	10
1.4 System Description .....	11
1.4.1 MDAV Wallet .....	11
1.4.2 MDAV Reader .....	12
1.4.3 MDAV Attribute Authority Administrative Portal .....	12
2.0 Tech Demo Design .....	14
2.1 Event Design .....	14
2.2 Facility .....	14
2.3 Limitations .....	14
2.4 Deviation from the Test Plan .....	15
3.0 Results .....	16
3.1 Application Feedback.....	16
3.1.1 User Identification .....	16
3.1.2 Market Information .....	16
3.1.3 Use Cases .....	16
3.1.4 Capabilities and Usability .....	17
3.1.5 Miscellaneous .....	18
3.2 Demonstration Survey.....	18
3.3 Conclusions.....	19
4.0 References.....	21



## LIST OF FIGURES

Figure 1-1 MDAV Wallet Storing Digital Capsules.....	12
Figure 1-2 Example of Attribute Authority Portal.....	13
Figure 3-1 Applicability of MDAV Survey Question Results .....	19
Figure 3-2 Usability of MDAV Survey Question Results .....	19

## LIST OF TABLES

Table 1-1 Actor Descriptions for Tech Demo.....	10
Table 1-2 Capability Matrix.....	10
Table 2-1 Personnel and Roles .....	14

## 1.0 INTRODUCTION

The National Urban Security Technology Laboratory (NUSTL) conducted a technology demonstration (tech demo) of Mobile Device Attribute Validation (MDAV) on December 11, 2018, to gather feedback from first responder end-users for the U.S. Department of Homeland Security (DHS), Science and Technology Directorate (S&T). MDAV is a mobile application that digitally authenticates first responders' credentials using X.509<sup>i</sup> public key cryptography on smartphones. MDAV aims to enable first responders to verify one another's credentials, permits and skill certifications quickly, securely and privately during field operations, even when there is no network connectivity. MDAV has two main mobile components: a wallet that contains cryptographically secure copies of certifications issued to a responder and a reader that validates those credentials when scanned. Credentials are relayed via several methods, such as Quick Response (QR) codes, near field communication (NFC) and Bluetooth. Additionally, there is a web application used by administrators (attribute authorities) to issue credentials.

The need for a technology that verifies responder's credentials came out of disaster responses, such as that to Hurricane Katrina, where responders set up perimeters to control access to scenes. Badges and other physical credentials are the current standard identification method, but they do not typically include specific information regarding the individual's training and certifications, and it is challenging to verify that they are authentic when the external agency is not known to the verifier.

To use MDAV, agencies issue cryptographic digital certificates (referred to as "data capsules") to their employees and representatives based on their roles and qualifications. For example, a hazmat technician's data capsule identifies them as trained to handle hazardous material. Upon arriving at a scene, an on-site field officer uses the MDAV reader to verify the authenticity of the hazmat technician data capsule by checking that the issuer is a recognized agency and that the responder can prove possession of the appropriate private key—a process that proves provenance.

MDAV is currently in the third phase of development, which entails performance testing and commercialization of the technology. Phase 1 was a viability test for the concept. Phase 2 involved initial execution and development of a minimum viable product. S&T asked for NUSTL's assistance in testing MDAV as part of the third phase.

Public key cryptography creates private and public keys used to sign digital artifacts. Individuals create private and public keys for signing capsules, which are X.509-based attribute certificates. Attribute authorities, known as certificate authorities in the X4.509 standards, use their own set of private and public keys to sign capsules. The attribute authority signature is an attestation of the validity of the credential contained within the capsule. Lockstep Technologies uses these properties of public key infrastructure (PKI) to wrap encapsulated, validated attributes (i.e., credentials) inside of digital certificates to more securely and privately convey data that is probably true.

---

<sup>i</sup> An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate [1].





Public key encryption works by creating a pair of functions that are the mathematical inverse of each other. One of the functions is kept secret (private key) and copies of the other function (public key) are given away freely. Any message the public key function is applied to will be jumbled, but applying the private key will reveal the original message. This also works in reverse (applying the private key to the message, and then using the public key to retrieve it). However, applying the same key twice will not reveal the original message.

## 1.1 PURPOSE

The purpose of this tech demo was to assist DHS S&T and its contracted developer, Lockstep Technologies, in gathering feedback from emergency response personnel on the concept and design of the MDAV application.

## 1.2 OBJECTIVE

This tech demo assessed:

- Overall concept
- Functionality for first responders
- Ease of use for all functions
- User interface
- Additional features required
- Confidence in the security and reliability
- Use cases

## 1.3 REQUIREMENTS

The requirements for the MDAV tech demo were captured in a capability matrix—presented in Table 1-1—that describes the roles involved in the tech demo. It includes the first responder who had the capsule, the field officers who verified it and the attribute authority administrators who issued it. Table 1-2 summarizes the capabilities that MDAV was expected to achieve and how they were tested during the demonstration.

Table 1-1 Actor Descriptions for Tech Demo

Actor	Description
First Responder	First responders use Mobile Device Attribute Validation (MDAV) to <b>request and manage data capsules</b> (credentials). They also use MDAV to <b>share capsules</b> with field officers to prove a credential.
Field Officers	Field officers use MDAV to <b>verify the data capsule</b> of a first responder before admitting them to an emergency scene.
Attribute Authority (AA) Administrator	The administrator is the person, working for the AA, who <b>validates the bona fide</b> and <b>issues the capsule</b> using the AA admin portal.

Table 1-2 Capability Matrix

Capability	Test Method
------------	-------------

<ul style="list-style-type: none"> <li>• FR can create profile on MDAV</li> <li>• FR can send a capsule request to one or more AA</li> </ul>	<ul style="list-style-type: none"> <li>• FR uses NUSTL test and evaluation smartphone to open the MDAV app to create their profile and sends the request</li> </ul>
<ul style="list-style-type: none"> <li>• AA can approve the capsule request</li> <li>• AA can deny the capsule request</li> </ul>	<ul style="list-style-type: none"> <li>• AA administrator uses a designated laptop to approve and/or deny the request</li> </ul>
<ul style="list-style-type: none"> <li>• FR can receive the approval</li> </ul>	<ul style="list-style-type: none"> <li>• FR uses the smartphone to open the MDAV wallet to receive approved capsules</li> </ul>
<ul style="list-style-type: none"> <li>• FO can use the MDAV reader to validate a FR's capsule</li> </ul>	<ul style="list-style-type: none"> <li>• FO uses the smartphone to scan the QR codes and validate the capsule</li> </ul>
<ul style="list-style-type: none"> <li>• AA can revoke the capsule</li> </ul>	<ul style="list-style-type: none"> <li>• AA administrator uses the designated laptop to revoke the capsule</li> </ul>
<ul style="list-style-type: none"> <li>• Capsules can be successfully validated with no network connectivity</li> </ul>	<ul style="list-style-type: none"> <li>• Both FR and FO disable WiFi and cellular connections and repeat the previous validation process</li> </ul>
<b>Notes:</b> AA - attribute authorities FO - field officer NUSTL - National Urban Security Technology Laboratory	
FR - first responder MDAV - Mobile Device Attribute Validation QR - quick response	

## 1.4 SYSTEM DESCRIPTION

MDAV verifies the credentials of first responders. Responder organizations issue capsules for their employees based on each responder's role and qualifications. Upon arriving at a scene, a field officer uses MDAV to verify the authenticity of the first responders' capsules by checking that the issuer is a recognized agency and that the responder presenting the certificate is in possession of the appropriate private key, verifying the provenance of the digital certificate. The following subsections describes the key system features that enable this capability.

### 1.4.1 MDAV WALLET

First responders use the MDAV wallet, pictured in Figure 1-1, to request new data capsules. This is done by pressing a button, selecting the appropriate organization or attribute authority, selecting a role and submitting the application. The application will then automatically create a private and public key pair, create a cryptographic signing request and then transmit it to the selected organization. An administrator at the organization will then review, validate and approve or reject the request.

The wallet also stores and manages the capsules. When a capsule is selected for sharing, it is transmitted to a field officer via QR code or Bluetooth. NFC is also being considered, and may be implemented in a future release.

### 1.4.2 MDAV READER

Field officers use MDAV reader to scan a data capsule and verify its contents. This verification includes:

- Verifying whether the data capsule is valid
- If the issuing authority is trusted
- If the role is acceptable
- If the provenance of the data capsule is valid.

Verifying provenance ensures that the individual holding the data capsule, the device and the issuing authority are all authentic. Once a field officer reads a data capsule and the first items are verified, the last step is to issue a challenge to the first responder. This challenge asks the responder to prove they are in possession of the capsule's private key. This process can be performed automatically if using the Bluetooth option, or via exchanging three QR codes, and proves the provenance of the data capsule to the field officer. The field officer is assured the individual, the device and the attribute authorities are authentic.

### 1.4.3 MDAV ATTRIBUTE AUTHORITY ADMINISTRATIVE PORTAL

MDAV includes an administrative web portal for attribute authorities, pictured in Figure 1-2. These are the organizations that first responders either work for or have relationships with. These organizations are the entities in a position to attest to the bona fides of a first responder.

The administrators are the only people who can login to the portal. Through the portal an administrator can do the following:

- Request Management
  - Approve or reject pending requests
  - Add comments to pending requests
  - View old requests.



Figure 1-1 MDAV Wallet Storing Digital Capsules

- Capsule Management
  - Revoke active capsules
  - View all capsules
  - Add comments to capsules.
- User Management
  - View capsules assigned to each other.

Admin Portal Local Organization 1 Share Export This week ▾

**Request Management**

Client	Request	Name	Role	Status
344	1541975874397	Adam Madlin	Paramedic	PENDING
344	1541881503206	Adam Madlin	Police_Commander	APPROVED
344	1541541677814	Adam Madlin	Firefighter_Chief	APPROVED
335	1540969845240	M P	Firefighter_Trainee	PENDING
334	1540895833025	Mukul P	Firefighter_Trainee	PENDING
333	1540891540018	M P	Emergency_Medical_Responder_(EMR)	APPROVED
333	1540891402921	M P	Police_Commander	APPROVED
333	1540887026338	M P	Firefighter_Trainee	APPROVED
332	1540797396284	Mukul Pande	Firefighter_Chief	APPROVED
332	1540797220516	Mukul Pande	Firefighter_Hazmat	APPROVED
332	1540797167150	Mukul Pande	Firefighter_Development	APPROVED
331	1540552677173	Mukul Pande	Mobile_Intensive_Care_Nurse_(MICN)	APPROVED
331	1540552722874	Mukul Pande	Emergency_Medical_Technician_(EMT)	APPROVED
331	1540552742942	Mukul Pande	Cardiac_Rescue_Technician-Intermediate	APPROVED
331	1540552765025	Mukul Pande	Mobile_Intensive_Care_Paramedic_(MICP)	APPROVED

First Previous 1 2 Next Last

Figure 1-2 Example of Attribute Authority Portal

## 2.0 TECH DEMO DESIGN

### 2.1 EVENT DESIGN

For this tech demo, three first responders from law enforcement and emergency management disciplines served as evaluators. The evaluators became familiar with MDAV and participated in various activities and group discussions. Data collectors from NUSTL were assigned to the evaluators and facilitated the test activities, recorded observations and comments throughout the event and gathered feedback from each evaluator following the completion of the event using a questionnaire. Observers were present to watch the activities of the tech demo.

### 2.2 FACILITY

The tech demo was conducted at NUSTL, located in a federal office building at 201 Varick Street in New York, New York. Introductions and discussion took place in the Grand Central conference room.

### 2.3 LIMITATIONS

Limiting factors to the design and execution of this tech demo included:

- **Authority, Training and Safety Regulations:** NUSTL’s standard operating procedures of participating agencies were followed. Participants did not perform tasks that created an unsafe work condition or went beyond their level of training or authority. Any participant could stop the tech demo if they encountered circumstances that created an unsafe work condition or observed an unsafe work act that could have led to an accident, injury, illness or adverse environmental impact. Participants were told to contact the NUSTL safety director or the NUSTL test director for resolution of any safety concerns.
- **Personal Information Protection:** The tech demo used simulated attributes and responder profiles. None of the participants’ personal information was used during the tech demo.
- **Scenario Realism:** The tech demo occurred under controlled conditions without the stress or stakes associated with a real disaster response. Evaluators extrapolated from the usability of MDAV in controlled conditions if they would be comfortable using it during an emergency response.

Table 2-1 lists the roles and organizations of key personnel for this tech demo.

Table 2-1 Personnel and Roles

Role	Organization
Test Director	Blaise Linn, NUSTL
S&T Support	Ryan Triplett, S&T Support Contractor

Role	Organization
Technology Developer	Les Chasen, Lockstep Technologies
Technology Developer	Steve Wilson, Lockstep Technologies
Technology Developer	Adam Madlin, Lockstep Technologies
Data Collector	Tyler Mackanin, NUSTL
Data Collector	Alaska Tran, NUSTL
Data Collector	Claire Gutekanst, NUSTL
Evaluator (Alpha)	NYCEM
Evaluator (Bravo)	NYPD
Evaluator (Charlie)	NYPD

## 2.4 DEVIATION FROM THE TEST PLAN

While the test was a success overall, there were several deviations from the test plan due to unforeseen circumstances. During the first break at approximately 10:45 a.m., evaluators Bravo and Charlie informed the test director that they had received a message from their commanding officer that their presence was required; they had to leave by noon. As a result, the overall test length had to be compressed by approximately three hours. The activities planned for the afternoon were replaced with a hands-on, table-top session. Evaluators were still able to test MDAV, but without the originally planned test scenario. Due to this, the simulated realism of the scenarios was not experienced by the evaluators, which could have affected their impressions of MDAV. Rather than being surveyed in person, the evaluators that left early were sent a copy of the questionnaire, which they answered and returned. Additionally, the discussion session was combined with the morning talks into a more open dialog. An additional feature of the app—Bluetooth credential exchange—was functional in the version used for the test, so participants were able to test it as well.

## 3.0 RESULTS

### 3.1 APPLICATION FEEDBACK

Throughout the tech demo, user feedback on all aspects of the application was collected. That feedback is categorized below.

#### 3.1.1 USER IDENTIFICATION

One major takeaway from the tech demo was honing in on the correct customer for the technology. While both responders and emergency management officials are the ultimate end users of the product, the evaluators were in agreement that the push to adopt MDAV and make it interoperable between agencies would come from the emergency management side.

The evaluators from the [New York City Police Department](#) (NYPD) felt that in the immediate aftermath of an emergency, responders would not have the time to verify credentials. Access control becomes stricter during sensitive cases, such as crime scene investigations. These evaluators agreed the application would be most useful when outside agencies need to be verified on a scene.

The [New York City Emergency Management](#) (NYCEM) evaluator made several recommendations concerning potential customers who could effectively use the technology. One suggestion was to contact the [Emergency Management Assistance Compact](#) (EMAC) committee. EMAC is the agency responsible for facilitating mutual aid between states and provides the legal basis for reciprocity of licenses and permits between states in a mutual aid scenario. Additionally, the [Incident Management Assistance Teams](#) (IMAT) were suggested as another possible federal partner who could encourage adoption.

#### 3.1.2 MARKET INFORMATION


Important market information was gained during the discussion. NYPD personnel currently have the ability to verify NYPD credentials using an app on their NYPD-issued phones. This only applies to NYPD personnel. The app essentially virtualizes NYPD identification cards.

This market information provided Lockstep Technologies with crucial information regarding the similarities and differences between their technology and an existing app already in use. A key difference between the two apps was found to be the ability to verify the legitimacy of credentials issued by outside agencies. The verification protocol methods were not compared due to a lack of information.

#### 3.1.3 USE CASES

An important point of discussion during the tech demo detailed potential use cases for responders and emergency management personnel. The NYPD identified the verification of credentials from outside agencies as the only use case for which their current app cannot





currently be used, so much of the discussion was focused on the emergency management use case, which was deemed more applicable overall. At an emergency scene, the incident commander needs to know who is coming to help and must verify qualifications and certifications for the aid they will provide. By verifying individuals' skillsets, they can better manage personnel resources and more effectively manage an incident scene. NYCEM thought MDAV's capabilities could be used to aid in resource management planning.


### **3.1.4 CAPABILITIES AND USABILITY**

Throughout the tech demo, evaluators posed questions to Lockstep Technologies concerning the functionality and design of MDAV that led to discussions regarding the capabilities and usability of the app. In addition, evaluators suggested additional capabilities they would find useful. An additional capability—the ability to send multiple credentials at the same time—was discussed; this could provide an incident commander with an index of the skillsets of all available personnel on scene. It was explained that often responders have training in areas other than the ones they were deployed for, which can be helpful if there is a shortage of a particular skillset.

The topics of record keeping and accountability in regard to emergency scenarios were discussed. NYCEM asked whether the reader phone stored the 'read' capsule data, and Lockstep Technologies noted that the app could store a record of this information in an audit log that is intended to be used in developing incident reports. NYCEM stated it would be beneficial to capture both the entry and leave times of responders during incidents to ensure and/or enforce that they are where they need to be.

For their purposes, NYPD wondered what would happen if a responder forgot to check-in with MDAV during an emergency incident, and how they would be accounted for in the audit log. They would not want to be penalized for forgetting to—or not having time to—check-in. Additionally, the NYPD thought the application may provide too much information and tracking that could lead to potential issues. Lockstep Technologies responded that data shared with outside agencies is limited to the credential ID number and attributes required to convey skills. Additional information would be in the database of the issuing agency but access could be restricted based on legitimate need. The evaluators discussed a hypothetical circumstance in which a responder's qualifications expired but their skillset was needed during the situation; they questioned if it would put the incident commander in a challenging position of having to refuse their assistance due to protocol, even though they knew the individual had been trained in the past and could carry out the task. Lockstep Technologies responded that MDAV is focused on providing high reliability data to incident managers to aid their decision-making, it does not remove their autonomy in making decisions.

After NYCEM stated they would like to limit the number of steps the individuals would have to go through in the field, Lockstep Technologies emphasized that all three steps using the QR code protocol were necessary to prove provenance. However, Lockstep Technologies was able to display MDAV's functionality via Bluetooth, which automates what occurs in the QR code process. In addition, NYCEM questioned whether the "valid thru" date of a capsule could be



extended. Lockstep Technologies stated this is possible by having a new capsule automatically requested when a capsule expires. The attribute authority could then determine if the credential is still valid and approve the request if appropriate. This would result in a new capsule with unique keys without requiring any action from the responder.

Another important piece of feedback that Lockstep Technologies received was that in a real scenario the incident commander would need to check in a large queue of responders. Therefore, they suggested the capability to validate multiple responder's credentials at the same time or in quick succession, rather than the current process. Lockstep Technologies said this modification would be possible using Bluetooth Low Energy to broadcast multiple capsules to one incident commander and indicated willingness to implement the idea. Additionally, NYCEM had the idea to expand MDAV's capabilities, or to integrate it into an existing system to attach capsules to mutual aid orders with specific qualifications/attributes needed in order to match individuals to an order and deploy resources effectively.

### **3.1.5 MISCELLANEOUS**

Aside from the feedback above, other suggestions and concerns were brought up during the discussions. NYCEM thought MDAV could be useful as part of a situational awareness system, and suggested looking to market leaders in incident management software to partner with and integrate the capabilities into existing software, such as the Federal Emergency Management Agency's (FEMA's) Web Emergency Operations Center-based Crisis Management System.

NYCEM thought the major challenge that the developers faced for adoption of their technology is the lack of standardization and baselining of qualifications across agencies. The underlying issue discussed was the differences between state, national and international standards and certifications that would need to be understood and trusted for the capsules to be trusted by a wide range of agencies. NYCEM suggested starting with FEMA's Resource Typing Library Tool to look at position qualifications, roles and certifications. It was also suggested that the vendor could implement the categories of the National Incident Management System as roles, though it was noted this might not necessarily map well to currently used terms in various states as it does vary across jurisdictions.

## **3.2 DEMONSTRATION SURVEY**

The demonstration survey asked participants a series of questions about the applicability and usability of MDAV. The survey followed a forced choice Likert scale; participants indicated if they: strongly agreed, agreed, disagreed or strongly disagreed with each question.

The results for applicability are shown in Figure 3-1 and support the comments about user identification. The NYPD participants largely disagreed with the statements about MDAV being useful for them specifically, but agreed it would be useful to other responders. The NYCEM participant indicated it would be useful for his organization. Figure 3-2 shows the usability metrics and supports the comments recorded in Section 3.1.4. All participants found MDAV easy to use over several metrics. Some participants chose not to answer questions about functions that were

only demonstrated, not part of the hands-on session. These are marked as “not tested” in the figure.

A complete copy of the survey given to evaluators along with their answers can be found in O.

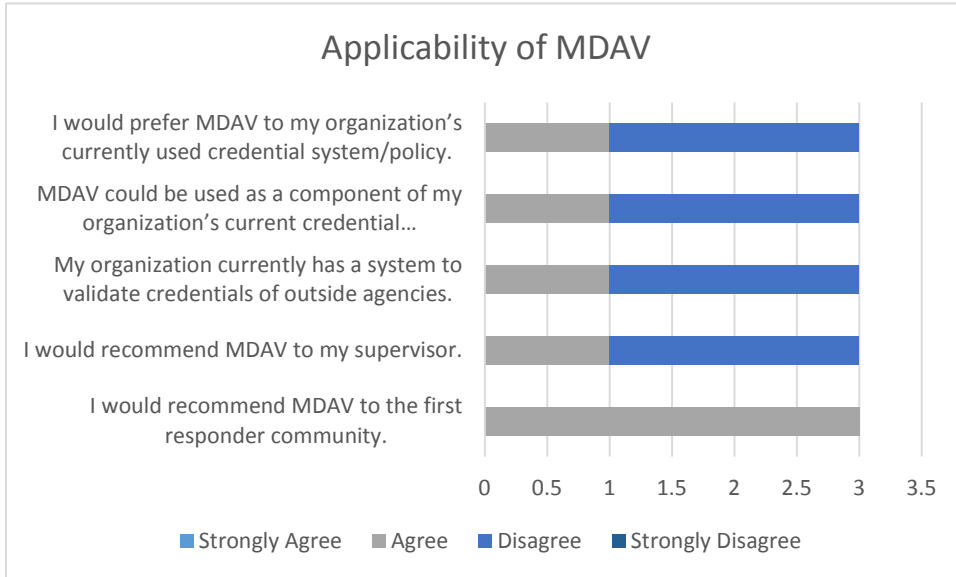


Figure 3-1 Applicability of MDAV Survey Question Results

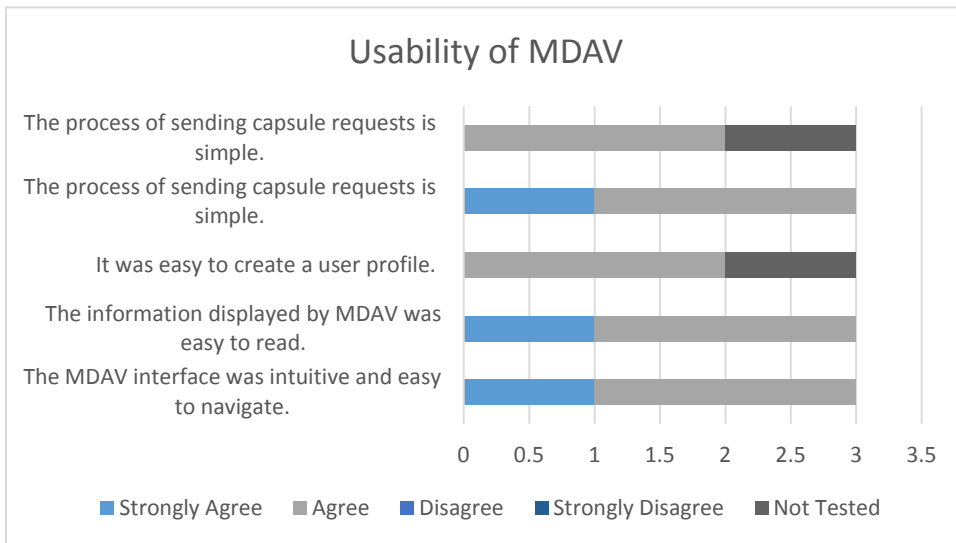


Figure 3-2 Usability of MDAV Survey Question Results

### 3.3 CONCLUSIONS

The objectives of the tech demo were to familiarize responders with MDAV and to collect feedback on the concept and design of MDAV. Overall, evaluators agreed on the ease of use of MDAV; however, evaluators believed that it should be acquired and adoption spearheaded by the



emergency management community, not directly by responder organizations. This was due to the fact that, on a daily basis, responders do not often deal with situations where they would have to verify another responder's credentials. The main applicable scenario is a mutual aid response, which is the purview of emergency management agencies and organizations.

NYCEM was interested in MDAV but described additional features that would make it more suitable for their use, such as adding the ability to transfer credentials from multiple responders at once to the incident commander, the ability to send more than one certification at once and the ability to view a list of responders with a particular skill at a scene.

Overall evaluators agreed a tool such as MDAV would be useful during large-scale responses that require the activation of mutual aid agreements.



## 4.0 REFERENCES

- [1] M. Rouse, "X.509 Certificate," January 2014. [Online]. Available: <https://searchsecurity.techtarget.com/definition/X509-certificate>.

## Appendix A. Survey Questionnaire Comments

Interface		Strongly Agree	Agree	Disagree	Strongly Disagree
The MDAV interface was intuitive and easy to navigate.	A	X			
	B		X		
	C		X		
<i>Comments:</i> A – The app was pretty easy to use; can go back and forth between screens easily. B – System was easy to use and very intuitive.					

Interface		Strongly Agree	Agree	Disagree	Strongly Disagree
The information displayed by MDAV was easy to read ( <i>display/font size/button size</i> ).	A	X			
	B		X		
	C		X		
<i>Comments:</i> B – It was easy to read and comparable to popular apps in style.					

Profile		Strongly Agree	Agree	Disagree	Strongly Disagree
It was easy to create a user profile.	A				
	B		X		
	C		X		
<i>Comments:</i> A – (N/A) Did not perform create a user profile first hand, but was shown how it would be done. B – Very easy to use.					



Capsule Request		Strongly Agree	Agree	Disagree	Strongly Disagree
The process of sending capsule requests is simple.	A	X			
	B		X		
	C		X		
<i>Comments:</i> <b>A</b> – The process seems simple; all you have to do is hit share. <b>B</b> – Simple to use.					

Capsule Approval		Strongly Agree	Agree	Disagree	Strongly Disagree
The process of approving a capsule request is simple.	A				
	B		X		
	C		X		
<i>Comments:</i> <b>A</b> – (N/A) Was shown the approval process, but was not done hands on. <b>B</b> – Simple to use.					

Capsule Verification		Strongly Agree	Agree	Disagree	Strongly Disagree
The capsule verification process is intuitive.	A	X			
	B		X		
	C		X		
<i>Comments:</i> <b>A</b> – It seems all you have to do is just click on share and connect via Bluetooth. Even the QR reader is easy, although the second step/scan is a pain—but it is logical. Thinks first responders would be able to figure it our easily. <b>B</b> – Very easy to figure out.					

Capsule Verification		Strongly Agree	Agree	Disagree	Strongly Disagree
The speed of verification is adequate for field operations. Time of verification process: N/A	A	X			
	B		X		
	C		X		
<p><i>Comments:</i>  <b>A</b> – The app was quick to call up and verify via Bluetooth, but police officers might not agree. For an emergency management case the app would need to be quick to process a lot of people in a line. Bluetooth is definitely fast enough and not as clunky as QR codes.  <b>C</b> – The speed is good unless there is an error that occurs. More time on the app would solve this problem.</p>					

App Performance		Strongly Agree	Agree	Disagree	Strongly Disagree
The application performs reliably.	A	X			
	B				
	C		X		
<p><i>Follow Up:</i> Did the application crash or freeze at any point during the demonstration?</p>					
<p><i>Comments:</i>  <b>A</b> – The app did not crash or freeze so it performed reliably.  <b>B</b> – (N/A) Unable to comment on this as we did not have enough exposure to the product.  <b>C</b> – App did crash in verification but was an easy fix just to resend the verification.</p>					

Usefulness		Strongly Agree	Agree	Disagree	Strongly Disagree
MDAV would be useful to my organization.	A		X		
	B			X	
	C			X	
<p><i>Follow Up:</i> How would the organization use MDAV?</p>					
<p><i>Comments:</i>  <b>A</b> – Could see it being used for out-of-state teams or on-scene teams to validate licensing. The tech is good and easy to use, but you need common standards to be trustworthy. Concern is not having common language in standards/trainings/certifications.  <b>B</b> – I can see a use for this in many organizations but not with ours. It would work for other first responders.  <b>C</b> – We already have something like this right now.</p>					



Overall Feedback		Strongly Agree	Agree	Disagree	Strongly Disagree
I would recommend MDAV to the first responder community.	A		X		
	B		X		
	C		X		
I would recommend MDAV to my supervisor.	A		X		
	B			X	
	C			X	
My organization currently has a system to validate credentials of outside agencies.	A		X		
	B			X	
	C			X	
MDAV could be used as a component of my organization's current credential system/policy.	A		X		
	B			X	
	C			X	
I would prefer MDAV to my organization's currently used credential system/policy.	A		X		
	B			X	
	C			X	
<p><i>Comments:</i></p> <p>A – Would prefer it as an add-on—might be better to just have everything in one box.</p> <p>C – This app would work better with an Office of Emergency Management-type of organization.</p>					
<p><b>What additional functions do you recommend be added to or removed from MDAV?</b></p> <p>A – Have the ability to have a little less secure shareable ‘token’ or QR code that can still convey reliable information. May not always want/need to do two-factor authentication for every task; add the ability to do one-factor as well, but under the same app.</p> <p>B – Unfortunately, we did not have enough exposure to this product to make this recommendation.</p>					
<p><b>What might stop your organization using MDAV?</b></p> <p>A – Procurement process, standards for certifications, lack of buy-in from cooperating agencies. Suggests targeting specific group with smaller amount of components or use incident management teams who have certification but no tech infrastructure.</p> <p>B – We have a similar system to verify internal members and verification of other agencies is done in other fashions. Electronic verification would take integration of secure services or information that some agencies may not want to share. I do see this as a possible useful tool for agencies that are base in inter-agency cooperation (e.g., Office of Emergency Management [OEM])</p> <p>C – Not really useful in day-to-day operations in my department. More useful for OEM type.</p>					