

Federated Identity, Credential, and Access Management Value Proposition Scenario: Public Safety Response to 2017 Hurricanes

BACKGROUND

In 2017, the United States and its territories were struck by three hurricanes within one month, causing widespread damage and affecting millions of people. Hurricane Harvey impacted 30 percent of the population in Texas, and Irma impacted 85 percent of the populations in Florida, Puerto Rico and the U.S. Virgin Islands. Maria impacted 100 percent of the populations in Puerto Rico and the U.S. Virgin Islands. These events caused communication outages and strained available public safety resources, creating dispatch and logistics challenges for responders and resulting in financial losses, injuries, and deaths that could have been avoided.¹

INFORMATION SHARING CHALLENGES

Public safety agencies faced multiple information sharing challenges that hindered response efforts, especially in Puerto Rico where Maria caused unprecedented destruction. The first challenge was cellular service disruptions, as catastrophic damage to Puerto Rico's cellular networks resulted in diminished voice communications. Vehicle-based cellular hotspots with satellite back-haul connectivity were established; however, these provided limited coverage to the ad-hoc assembly of first responders on the ground and proved insufficient to meet real-time public safety communication needs. The second challenge was the inability of dispatchers to communicate effectively with responders via computer-aided dispatch (CAD) systems. While Puerto Rico received more than 300 emergency services vehicles (fire, police, ambulance and power) from the U.S. mainland, the CAD systems in these vehicles could not interoperate with CAD systems local to Puerto Rico. The sporadic connectivity provided by hotspots could have allowed use of non-voice communications such as CAD messaging, but dispatchers were largely unable to direct first responders to critical response areas in a timely manner due to these CAD interoperability challenges.



POTENTIAL FOR FEDERATED IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

The response to Maria and the other 2017 hurricanes could have been more effective through interoperable, trusted communications among the CAD systems used by participating public safety agencies. Such CAD-to-CAD communications capabilities could have enabled local dispatchers to send secure, trusted dispatch messages to responders in affected areas. Enabling such communications across CAD applications requires new ways of thinking about trust and interoperability for CAD vendors and public safety agencies. Stakeholders must embrace emerging technologies and capabilities such as federated trust frameworks and trusted Federated ICAM and implement CAD systems that are natively capable of authenticating federated users and trusting and interoperating with other CAD systems across jurisdictional boundaries.

¹ 2017 Hurricane Season FEMA After-Action Report. Federal Emergency Management Agency. <https://www.fema.gov/media-library-data/1531743865541-d16794d43d3082544435e1471da07880/2017FEMAHurricaneAAR.pdf> (accessed July 1, 2020).

HURRICANE VALUE PROPOSITION

- Enhance CAD Messaging to support alternative non-voice communications
- Enable dispatchers to communicate effectively with responders via CAD systems
- Design new ways of thinking about trust and interoperability for vendors and public safety
- Share Response Plans in advance of an incident

SAFECOM AND THE NATIONAL COUNCIL OF STATEWIDE INTEROPERABILITY COORDINATORS

SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) recognize the vast potential of Federated ICAM to improve public safety information sharing, and they also recognize the lack of clear Federated ICAM implementation guidance available to public safety agencies today. In response, they are developing a new framework of Federated ICAM implementation tools and guidance that will enable public safety agencies to reap the tremendous potential benefits that Federated ICAM can provide.



Five major components of a successful ICAM program.

TRUSTMARK FRAMEWORK

The proposed solution SAFECOM and NCSWIC are developing is based on an emerging technology called “trustmarks.” Trustmarks will enable agencies to quickly and easily discover and define the policy requirements for their information sharing use cases in a transparent, standard way. Trustmarks also will enable agencies to quickly and cost-effectively demonstrate that their personnel and applications comply with those requirements. This framework can be integrated into existing information sharing applications and future applications quickly and cost-effectively. When it is available, this framework will provide a clear and cost-effective path for agencies to develop trusted information sharing relationships and implement trusted information sharing systems that will lead to more effective mission outcomes across the entire public safety community.

VISION FOR TRUSTMARKS

- Standardize policy requirements
- Information sharing transparency
- Cost-effective solution
- Leverage existing identity credentials
- Ease of integration