Federated Identity, Credential, and Access Management Value Proposition Scenario: Public Safety Response to Drug Epidemics

BACKGROUND

Drug overdoses and addiction-related problems have become considerable challenges nationwide. According to the Centers for Disease Control and Prevention (CDC), over 65,000 people died in 2018 from drug overdoses in the United States.[1] Opioid overdoses are particularly troublesome, as the majority of overdose deaths (70 percent) involved opioid use.[2] In Tennessee, drug overdose deaths have surpassed traffic fatalities. On average, nearly five people die every day in Tennessee from a drug overdose, and most of these deaths are associated with opioids.[3] The problem is widely recognized by physicians nationwide, and as a result, the CDC reports a decrease in the number of opioid prescriptions written from 2012 to 2018.[4] Despite this trend, drug crime, treatment, and overdose deaths during the same time period have increased due to illicitly synthesized and distributed opioids, such as heroin and fentanyl, as well as a resurgence of methamphetamine and cocaine use.[5]

INFORMATION SHARING CHALLENGES

The public safety community has two primary responsibilities in combating the drug and opioid epidemics: first, emergency response services (EMS) assist overdose victims; second, law enforcement investigate and shut down illegal production and distribution. The information sharing capabilities required to carry out these responsibilities effectively are quite sophisticated, requiring cooperation among hospital emergency departments, medical examiners, drug treatment facilities, EMS responders, EMS dispatchers, and law enforcement personnel. These groups must share many different types of information, doing so in a manner that respects the laws and regulations pertaining to this information, which can be challenging. A person who suffers an overdose can be a patient, a victim, a suspect, a criminal, or all of the above. These differing outlooks on the epidemic can lead to different goals and information sharing priorities that further complicate the information sharing challenge.

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

Many public safety stakeholders throughout the U.S. have recognized the inherent complexity of drug overdose information sharing, and some have even developed systems and applications to address the problem. Below are three examples of such developments (as of July 2020):

- The El Paso Intelligence Center (EPIC) has a pilot project named DOTS (Drug Overdose Tracking System), with a goal of collecting health and law enforcement information and then sharing it with law enforcement
- The Baltimore High Intensity Drug Trafficking Area (HIDTA) has implemented a system called ODMAP (Overdose Detection Mapping Application Program) for collecting and disseminating select drug trafficking information

[1] *Drug Overdose Deaths.* Centers for Disease Control and Prevention. Last reviewed March 19, 2020. https://www.cdc.gov/drugoverdose/data/statedeaths.html (accessed July 2, 2020).

[2] *Drug and Opioid-involved Overdose Deaths—United States, 2017-2018.* Centers for Disease Control and Prevention. March 20, 2020. https://www.cdc.gov/drugoverdose/data/statedeaths.html (accessed July 2, 2020).

[3] Tennessee Deaths from Drug Overdoses Increase in 2017. Tennessee Department of Health. August 20, 2018. https://www.tn.gov/health/news/2018/8/20/tennessee-deaths-from-drug-overdoses-increase-in-2017.html (accessed July 2, 2020).

[4] Ibid.

[5] Ibid.

- Tennessee is implementing multiple such systems, including its Drug Investigation & Information Integration (DI3) system (currently in use) and a more ambitious Data Warehouse Initiative (still under development)

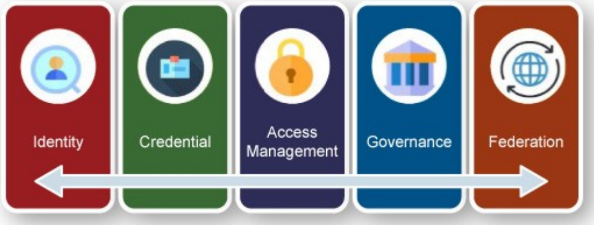
All of these systems have the potential to improve information sharing to combat the opioid or other drug epidemics; however, any system must satisfy two critical requirements. First, they must enable collaboration between stakeholders that span multiple agencies, communities, and jurisdictions. Second, they must respect the sensitivity of the data and enforce appropriate laws and regulations related to its distribution. Collecting, maintaining, and sharing sensitive data among a large group of diverse users is difficult. Managing users and access levels within a system can be complex and costly, since authorized users can come from many different types of organizations. Users must be properly vetted and attested for the system and its data to be trusted. The data needs to be accessible, but also secure and trusted. Federated ICAM is a critical enabler of many types of data sharing systems and applications that span multiple agencies and communities. Under a Federated ICAM approach, authorized users can log into information sharing systems and applications using their existing authentication credentials issued by their home agencies or organizations. Access to sensitive data can be managed through trusted attributes provided on behalf of users by their home agencies or organizations. This solution reduces cost burden while also improving security.

DRUG OVERDOSE VALUE PROPOSITION

- Ability to share different types of information must comply with laws and regulations
- Collaboration between stakeholders will span multiple agencies, communities, and jurisdictions
- Ability to support authorized users from many different types of organizations

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