Title: District Interoperable PIV-I PACS System (DIPPS)

Category: Cybersecurity

State: District of Columbia – Office of the Chief Technology Officer (OCTO)

Contact: Michael Rupert – OCTO Communications Director, Michael.rupert@dc.gov

Office: 202-724-5178, **Mobile:** 202-657-3831

Project Start Date: January 2016

Website: http://octo.dc.gov

EXECUTIVE SUMMARY

The District Interoperable PIV-I PACS System (DIPPS) is an optimized secure credential that offers interoperability among federal, state, local, and commercial entities. Through the use of Extensible Access Control Markup Language (XACML), DIPPS innovatively delivers “first-in-its-class” physical and logical access to facilities and systems.

PROJECT NARRATIVE

Concept

The September 2013 Washington Navy Yard shooting underscored credentialing reliability's importance. Hindsight never changes security breaches but innovation can. To this end, the Office of the Chief Technology Officer (OCTO) and the District of Columbia Homeland Security & Emergency Management Agency (HSEMA) developed the District Interoperable PIV-I PACS System (DIPPS).

Supported by District of Columbia Mayor Muriel Bowser, Chief Technology Officer Archana Vemulapalli, HSEMA Director Chris T. Geldart, and OCTO and HSEMA's groundbreaking solution directly accounts for increasing vulnerabilities and credentialing interoperability needs. In moments, DIPPS allows visitors to present their credentials, have the card PIN verified and electronically validated. These security measures exceed visual inspections and offer heightened security. Individuals can also receive as-needed building access, which enhances emergency resource management.

To our credit, DIPPS is the first to use Extensible Access Control Markup Language (XACML) to control physical and logical access against a single enterprise Identity and Access Management System (IAM) platform using a standards-based message. Traditional Physical Access Control Systems (PACS) make access decisions by sending non-standard access request messages to proprietary turnkey PACS. Value-added system features include certificate validation against the Federal PKI bridge during enrollment. The capability to perform a certificate challenge or response, at each card read, is also valuable.

Significance

The September 11 attacks laid the foundation for DIPPS. The October 2001 series of Homeland Security Presidential Directives (HSPD) established a national strategy to safeguard the country and respond to future attacks. HSPD-12 -- created on August 27, 2004 -- called for U.S. policy to establish Government-wide identification standards. The PIV-I card was then designed to follow the FIPS-201 policy, which defines federal employee and contractor common identification requirements. This solution, however, did not address the need for interoperability and shared trust among non-federal agencies and federal government PIV/CAC systems.

Alternatively, DIPPS introduces a substantially new technology that allows PACS to decide on card validations against the Central Identity Management System instead of the proprietary turnkey PACS. The capacity to perform certificate challenges to validate authority creates that certificate “chain of trust,” which can be crossed over to the federal bridge. The DIPPS team utilized the Iterative Software Development Life Cycle for the project management; the project cost was $439,400.Utilizing this model, the iterative process begins by applying a small set of the DIPPS software requirements and iteratively enhancing the evolving versions until the complete system is applied and ready to be deployed.

Proof of concept was realized during the March 2016 Nuclear Security Summit (NSS). NSS deployed DIPPS for testing, enrolling, and issuing the PIV-I and CAC card for physical participant access at HSEMA among all levels of state, local, federal, and commercial agencies. Visitors were successfully granted HSEMA Visitor Lobby advance-access via email invitation and the Just-In-Time (JIT) PACS on-site registration.

DIPPS is an innovative government program that mirrors NASCIO's principles. First, our system introduces a governance framework that shifts the DC Department of General Service's total oversight to a governance framework that now includes HSEMA and OCTO. This development improves accountability and interoperability by allowing trusted, federal credentials to authenticate at the District's HSEMA and OCTO's facilities. This augmentation permits physical access to the building and logical access to systems. DIPPS creates a solution in which access decisions are made against the District's Central IAM versus a proprietary turnkey Physical Access Control System (PACS). HSEMA and OCTO can now respectively maintain ownership and accountability of access management to their facilities.

Impact

This initiative is distinguished by quantifiable results, which are the true marker of an innovation's success. During the Nuclear Security Summit of 2016, District, federal and defense emergency operations activities to support the event were held at HSEMA. Multiagency team members were able to seamlessly and securely access the facility using their own CAC, PIV, and PIV-I credentials. DIPPS' effectiveness accounts for a 75 percent decline in the number of visitors processed via the less secure, manual security screening system.

Moreover, the JIT PACS registration is an added solution benefit. This feature permits FIPS-201 validated cardholders to be quickly registered and enrolled during emergency events where collaboration among state, local, and federal agencies is mission-critical. The JIT access allows authorized individuals -- who have not pre-registered for facility access -- to register and enroll at the door. JIT access can be self-administered at self-service kiosks, where practical. Within 3 minutes or less, guests can bypass visitor lines to access a secure facility. Our stylized solution gives first responders and emergency personnel the authority needed to fully execute public safety measures in the shortest, most efficient timeframe. In another instance, HSEMA federal partners evaluated DIPPS during the January 2016 State of the Union Address. Its utilization for these events has cumulatively diminished facility access and interoperability problems by 96 percent.

These highlights affirm how easily the design can be transferred and replicated among government entities. DIPPS is fully able to serve as a model for other jurisdictions. It clearly adheres to industry standards and offers proven interoperability between federal PIVs, military CACs, and other jurisdictional PIV-I cards.

Next-level uses of DIPPS will include logical, smartcard access to network environments and applications. The breadth and scope of our innovation will also enhance any discipline or policy area (e.g., health and human services) that requires high-assurance identity vetting and access management.

The DIPPS' demonstrated commitment to information technology inclusion aligns with the NASCIO State IT Recognition Awards mission. These qualifications make the DIPPS innovation an ideal award recipient.