Identity, Credential, and Access Management (ICAM) Common Appendices

Science and Technology Directorate

Homeland Security

Science and Technology

Primary Authors

Christine Owen

Larry Kroll

Chris Price

David Shapiro

Contributing Organizations

Oasys International Organization

Department of Homeland Security (DHS) Science & Technology Directorate

Partner Engagement-Information Sharing Environment (PE-ISE)

DHS Office of Emergency Communications (OEC)

First Responder Network Authority (FirstNet)

Federal Communication Commission (FCC)

National Institute for Science and Technology Public Safety Communications Research Division (NIST PSCR)

PUBLIC SAFETY COMMUNICATIONS

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

WORKING GROUP

Identity, Credential, and Access Management (ICAM) Common Appendices

April 2018

Version 1

Prepared for

Department of Homeland Security

Science and Technology Directorate

CONTENTS

1 APPENDIX A: ICAM DEFINITIONS

Service Area and Functions

Source: GSA FICAM Architecture at idmanagement.gov

Access Management: The ability to allow only permitted individuals to access a certain computer system.

Access Policies: The rules around who can get to resources, and when.

Assertions: The ability to provide secure assertions that: testify to an attribute of an individual or an authentication or authorization decision made by another party in a secure manner; protect the privacy of an individual; can be trusted and understood by a relying party; and interoperate with the systems of a relying party.

Attribute-Based Access Control (ABAC): Access control measures automated through attributes and access rights given to users.

Authentication: The ability to confirm that a physical person attempting to access resources is who they claim to be.

Authorization: The set of practices around (1) provisioning users' access to certain resources and (2) providing users with access to those resources to which they have been provisioned access when requested.

Credential: Authoritative evidence of an individual's claimed identity. Binds an identity (and optionally, additional attributes) to an authenticator (i.e. card, memorized password, etc.) possessed and controlled by a person.

Credential Issuance: The ability to physically issue authenticators to individuals and attach an individual's digital identity to a credential.

Credential Maintenance: The ability to maintain this credential over time to ensure the integrity, and protection of the information it contains; the ability to prevent any fraudulent activity around the use of the credential; the ability to renew credentials and handle incidents pertaining to lost or compromised credentials.

Credential Management: The set of practices required to establish and maintain a credential over its lifecycle, and to provide authentication services for credentials.

Credential Registration: The ability to register an individual and their associated digital identity to receive a credential.

Credential Revocation: The ability to invalidate a credential.

Credential Sponsorship: The process of accepting a recommendation for an individual to be issued a credential.

Federation: The ability of one organization to accept another organization's work (i.e., identity proofing, credentials or authorization) based on inter-organizational trust.

Identifier: A unique attribute that can be used to locate a specific identity within its context.

Identity: The set of characteristics (also called "attributes") that describe an individual within a given context.

Identity Creation: The ability to create a unique digital representation of an individual's unique identity including all necessary attributes.

Identity Deactivation: The ability to terminate a digital representation of an individual's identity.

Identity Maintenance: The ability to maintain this digital representation over time to ensure the accuracy, integrity and protection of the information it contains, reflecting any necessary changes or updates.

Identity Management: Consists of the set of practices required to establish and maintain a digital identity over its lifecycle.

Identity Proofing: The ability to prove the identities of individuals to establish confidence that the individual is who they claim to be.

Identity Resolution: The ability to identify duplicate digital identities.

Infrastructure: The architecture and implementation of Resource Owner ICAM hardware and software.

IT Shared Service: An information technology function that is provided for consumption by multiple organizations within or between federal agencies, state, local, tribal, territorial and private sector entities.

Multifactor Authentication: An authentication method that requires the use of two of three "factors": something you have (a credential), something you are (fingerprint) and something you know (password).

Payload: The semantic and syntactic structure of the data exchanged between the Resource Owner and partner systems.

Policy: The standards/requirements documents that govern Resource Owner practices.

Privacy: The privacy measures necessary to protect end-user privacy based on an assessment of risk.

Procedures: The procedures the Resource Owner follows to implement and adhere to policy.

Protocol: The communications method and interface between Resource Owner systems and partner systems.

Resource Tagging: The labeling of resources with the appropriate metadata values so that they can be sorted according to the access policy, ensuring only the right resources are accessed by the right people.

Risk: The risks pertaining to the access or breach of Resource Owner resources or end-user personal information.

Single Factor Authentication: Using one factor (i.e., username and password) to enter a computer system; this is a weaker form of protection for computer systems and applications.

Trust Framework: A collection of standards and requirements that govern the trust between two or more organizations within the trust framework.

Security: The security measures necessary to protect Resource Owner resources and end-user personal information based on an assessment of risk.

Verification: The set of practices required to provide secure assertions that testify to an attribute of an individual or an authentication or authorization decision made by another party.

2 APPENDIX B: ACRONYM TABLE

Acronym	Description
AAS	Authoritative Attribute Service
ABAC	Attribute Based Access Control
AL	Assurance Level
AAL	Authentication Assurance Level
APL	Approved Products List
BJA	Bureau of Justice Assistance
COMMUNITY	Public Safety Community
CybOX	Cyber Observable Expression
DHS	Department of Homeland Security
E-PACS	Enterprise Physical Access Control System
FAL	Federal Assurance Level
FAR	Federal Acquisition Regulation
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
GFIPM	Global Federation Identity and Privilege Management
GSA	General Services Administration
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
ID	Identity Document
IDP	Identity Service Provider
IT	Information Technology
LDAP	Lightweight Directory Access Protocol

Acronym	Description
NGFR	Next Generation First Responder
NIST	National Institute of Standards and Technology
OJP	Office of Justice Programs
PE-ISE	Partner Engagement-Information Sharing Environment
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Policy Information Point
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKI	Public Key Infrastructure
PHI	Protected Health Information
PM-ISE	Program Manager for the Information Sharing Environment
PSC ICAM WG	Public Safety Communications Identity, Credential and Access Management Working Group
RBAC	Role Based Access Control
REST	Representational State Transfer
RFI	Request for Information
RFP	Request for Proposal
S&T	Science and Technology Directorate
SAML	Security Markup Language
SBU	Sensitive But Unclassified
SICAM	State Identity, Credential, and Access Management
SLA	Service Level Agreement
SLTT	State, Local, Territorial, and Tribal

Acronym	Description
SME	Subject Matter Expert
SOW	Statement of Work
SP	Service Provider
SSO	Simplified Sign On
STAC	Sensitive But Unclassified Technical Advisory Council
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
TFP	Trust Framework Provider
xAL	combined Assurance Levels

3 APPENDIX C: NORMATIVE REFERENCES

- Enabling Strong Authentication with Personal Identification Verification (PIV) Cards: Public Key Infrastructure (PKI) in Enterprise Physical Access Control Systems (E-PACS) Recommended Procurement Language for RFPs.

  Retrieved from: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/Procurement-Language-1.1.0.pdf

- Federal Trust Services List

  Retrieved from: https://www.idmanagement.gov/trust-services/

- GSA Approved Products List (APL)

  Retrieved from: https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage

- PM-ISE Introduction to ICAM Principles – Identity, Credential, and Access Management Brochure

  Retrieved from: https://www.dni.gov/files/ISE/documents/DocumentLibrary/INTRO-TO-ICAM.pdf

- NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*

  Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- Federal Information Processing Standard (FIPS) Publication 140-2: *Security Requirements for Cryptographic Modules*

  Retrieved from: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

- Subpart 27.4 – *Rights in Data and Copyrights* of the Federal Acquisition Regulation (FAR)

  Retrieved from: https://www.acquisition.gov/?q=browse/far/27/4&searchTerms=data%20rights

- NIST SP 800-63-3: *Digital Identity Guidelines*

  Retrieved from: https://pages.nist.gov/800-63-3/sp800-63-3.html

- Federal Identity, Credential, and Access Management Guidance and Roadmap (FICAM)

  Retrieved from: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf

- State Identity, Credential, and Access Management Guidance and Roadmap (SICAM)

  Retrieved from: http://www.nascio.org/Publications/ArtMID/485/ArticleID/161/The-State-Identity-Credential-and-Access-Management-Guidance-and-Roadmap-SICAM

- M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007

  Retrieved from: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

- NIST SP 800-162: *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

  Retrieved from: http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

- The NIST Model for Role Based Access Control: Towards a Unified Standard (2000)

  Retrieved from: https://www.nist.gov/publications/nist-model-role-based-access-control-towards-unified-standard

- DHS Grant Resources

  Retrieved from: https://www.dhs.gov/how-do-i/find-and-apply-grants

- Grants.gov

  Retrieved from: www.grants.gov

- Bureau of Justice Assistance (BJA)

  Retrieved from: https://www.bja.gov/funding.aspx

- Office of Justice Programs (OJP)

  Retrieved from: https://ojp.gov/funding/

- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework

  Retrieved from: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/Common-Policy-Framework.pdf

- SAFECOM / NCSWIC ICAM 101 Briefing for Public Safety Officials

  Retrieved from: https://www.dhs.gov/safecom/icam-resources