Credential Management (CREDMGMT) Overview

June 15, 2017
12:00 pm – 1:00 pm EST

CDM

A CDM LEARNING COMMUNITY EVENT

Today's Webinar Goals

1. Describe Continuous Diagnostics and Mitigation (CDM) Phase 2 "Who is on your network?"
2. Present an overview of CREDMGMT and its core concepts
3. Outline important agency CREDMGMT considerations

We'll Answer These Questions

- What is CREDMGMT?
- Why do we need CREDMGMT?
- How does CREDMGMT fit into the overall CDM effort?
- How does CREDMGMT support Identity, Credential, and Access Management (ICAM)?
- What is the agency role in the CREDMGMT solution?

Today's Speaker: Ross Foard

PMP, CISSP, CIAM, ITIL

- CDM Phase 2 Engineer and ICAM subject matter expert (SME)
- Re-joined the U.S. Department of Homeland Security (DHS) in 2016
- Expertise in identity management, strong authentication, Personal Identity Verification (PIV) cards, access management, and account management

Basics of CREDMGMT

- Addresses strong authentication of unprivileged users on the network
- Tightens polices and practices for network users
- Preferred PIV card use for accessing agency networks
- Is part of CDM Phase 2 that procures tools, sensors, and services to implement aspects of credential management, a key activity of the CDM Phase 2 program

CDM

Why We Need CREDMGMT

- Over 60% of confirmed data breaches involved **weak, default, or stolen passwords**.
- The use of **stolen credentials** targeting traditional username and password authentication is prevalent across numerous cyber attack patterns.
- Several of the top hacking action varieties and malware functionalities continue to target **static credentials** in the form of usernames and passwords.

Source: 2016 Verizon Data Breach Report

Policy CREDMGMT Supports

- **Cybersecurity Strategy and Implementation Plan (CSIP), October 2015:** "All agencies will improve the identity and access management of user accounts on Federal information systems to drastically reduce vulnerabilities and successful intrusions."
- **Cybersecurity Sprint Memo, June 2015:** "Intruders can easily steal or guess usernames/passwords and use them to gain access to Federal networks, systems, and data. Requiring the utilization of a Personal Identity Verification (PIV) card or alternative form of multi-factor authentication can significantly reduce the risk of adversaries penetrating Federal networks and systems…"

Programs/Standards CREDMGMT Supports

- **Identity, Credential, and Access Management (ICAM)** – Incorporates ICAM architectural elements and focuses on strong authentication leveraging the PIV card
- **Federal Information Processing Standard Publication 201 (FIPS 201)** – Specifies PIV requirements
- **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2** – Describes electronic authentication and level of assurance (LOA)

CREDMGMT & CDM Implementation

- The CDM Program uses Privilege Access Management (PRIVMGMT) and CREDMGMT as mechanisms to get products and services for critical CDM capabilities.
- Integration into CDM dashboard (e.g., metrics and reporting) will be provided at a later time.
- A partnership of ICAM and CDM functions within an agency is critical for the success of this effort.

CDM Phase 2 Tool Functional Areas (TFAs)

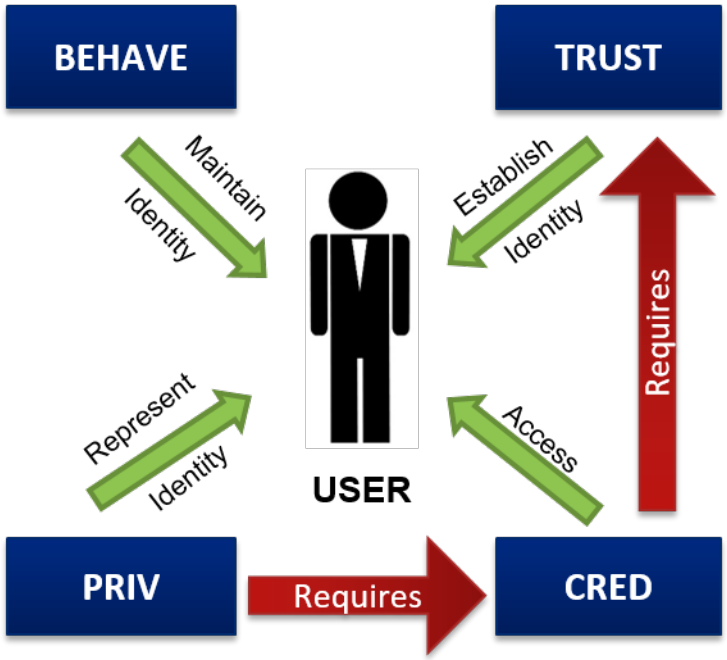
- **Manage Trust in People Granted Access (TRUST) – Were users properly vetted?**
- **Manage Security Related Behavior (BEHAVE) – Have users been trained?**
- **Manage Credentials and Authentication (CRED) – Are users accessing the network with PIV cards?**
- Manage Privileges (PRIV) – What access do administrators have (under PRIVMGMT)

CRED Tool Functional Area

- Reduces probability of loss in availability, integrity, and confidentiality of data
- Ensures credentials for physical and logical access are assigned to and only used by authorized users who require access to perform their job duties
- Key concepts:
  - **Master User Record (MUR)** – Elements of CRED are contained in a MUR
  - **Policy Decision Point (PDP)** – Compares the desired state with the actual state to determine if they are in alignment
  - **Policy Enforcement Point (PEP)** – Relies on Active Directory policy for enforcement of Network Logon

CDM Phase 2 – Credential Management

TRUST, BEHAVE, CRED and PRIV
Relationship to the User



USER is a generic term that applies to any entity (including non-person entities) that access any resource, physical or logical, in an organization.

TRUST is used to validate a person's identity and the degree to which they have been vetted.

CRED is a digital representation of a user and binds a type of credential or authentication mechanism to an identity established in TRUST with a level of assurance and is used to grant access (physical and logical).

PRIV establishes the privileges associated with the credential and in turn the individual or service

BEHAVE identifies that the individual has the proper knowledge and training for the roles they are assigned and that they remain up to date.

Master User Record Data

- The MUR will contain key attributable data from the CRED, PRIV, TRUST, and BEHAVE capabilities to support CREDMGMT:
  - TRUST – Validates a person's identity (ID Proofing) and the degree to which they have been vetted (Suitability)
  - BEHAVE – Validates a user has the proper knowledge and training for the role they have been assigned (Cyber Security Annual Training)
  - CRED – Binds the credential and authentication mechanism to an identity established in TRUST with the appropriate LOA (PIV credentials)
  - PRIV – Establishes the privileges associated with the credential to assess target devices (under PRIVMGMT Task Order)
- CREDMGMT is **highly dependent** on each Phase 2 capability for success (e.g., cannot have proper CRED without TRUST).

Policy Decision Point

- PDP implements machine readable policies; rules that control access/operations and are ideally machine readable and executable.
- PDP compares policy with as-is attributes to which will allow CDM Dashboard to calculate defects.
- Dashboard integration will be in a future task order under CDM.
- For example, CDM theoretically could inform a chief information security officer (CISO) of a User who has been granted network access without utilizing the PIV card.

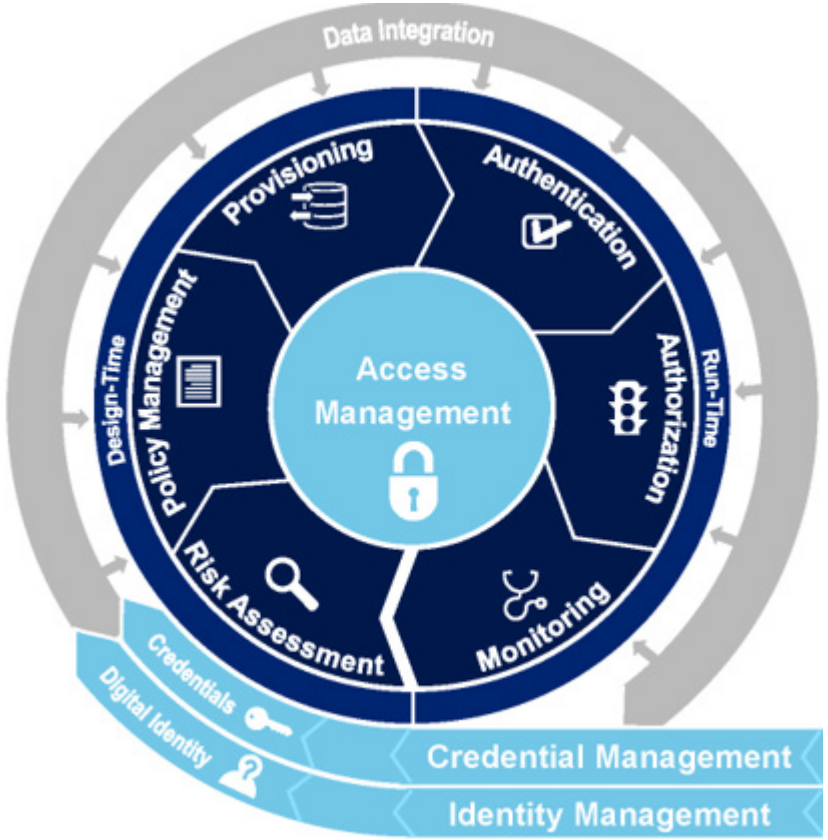
MUR and PDP – SailPoint

CDM Functional Area	Target Attributes	Target Data Sources
TRUST	• A common identifier for all privileged users • The manager of the privileged user • Whether or not the user has a valid PIV assigned	• Agency-specific
BEHAVE	• Whether or not the user has taken annual security training • Whether or not the user has taken any additional training required for privileged users	• Agency-specific • Learning Management Systems or flat file
CRED	• Does the user have a credential assigned? (includes PIV and other credential types) • If credential type is not PIV, does it meet complexity requirements? • Does the credential meet age requirements? • Are other accounts entitled to use the same credential?	• Active Directory, LDAP, Agency-specific
PRIV (from PRIVMGMT)	• To which credentials does an Administrator use to access credential vault? • To which target devices does an Administrator have access to?	• Active Directory, LDAP, Agency-specific

How CREDMGMT Supports ICAM

Supports ICAM through strong authentication leveraging the PIV card. Key concepts for ICAM include the following:

- **How a user is authenticated** – CREDMGMT will focus on network access at desktop
- Measure how **suitability** is performed to support the PIV card (TRUST)
- Measure if **Cyber Security training** has occurred to inform users how to take actions to mitigate risks.



User Authentication

Authenticate a user

This use case describes, in detail, the steps for authenticating a user who has requested access to a protected resource. It stems from the 'Grant access to a protected resource' use case and expands on Step 3, 'Verify authentication factors.'

Authentication is the process by which a system verifies the user's claimed identity to a certain level of assurance (LOA). LOA1 is the lowest level, and LOA4 is the highest.

There are three types of authentication factors: **** something you know (such as a password or PIN), something you have (such as a smartcard), and something you are (such as your fingerprint). At LOA3 and LOA4, at least two types of factors are required.

Actors & Systems Key

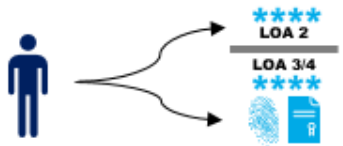
- Individual
- Credential
- Protected resource
- Access Control System (ACS)

Precondition: Individual has attempted to access a resource.

1. Prompt for Authentication

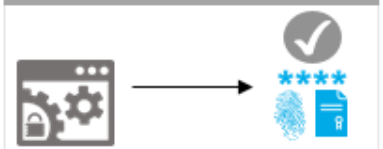
- The Access Control System (ACS) prompts the individual to provide authentication factor(s).

2. User Input



- For LOA 2, the individual provides a single authentication factor, usually a PIN or password.
- For LOA 3 and LOA 4, the individual provides at least two authentication factors.

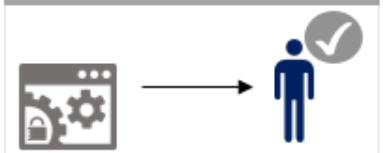
3. Input Verified



- The ACS verifies the user's input against information about the user's claimed identity.

Each type of factor is authenticated in a different way.

4. User Authenticated



- If the factors are verified, authentication is successful.

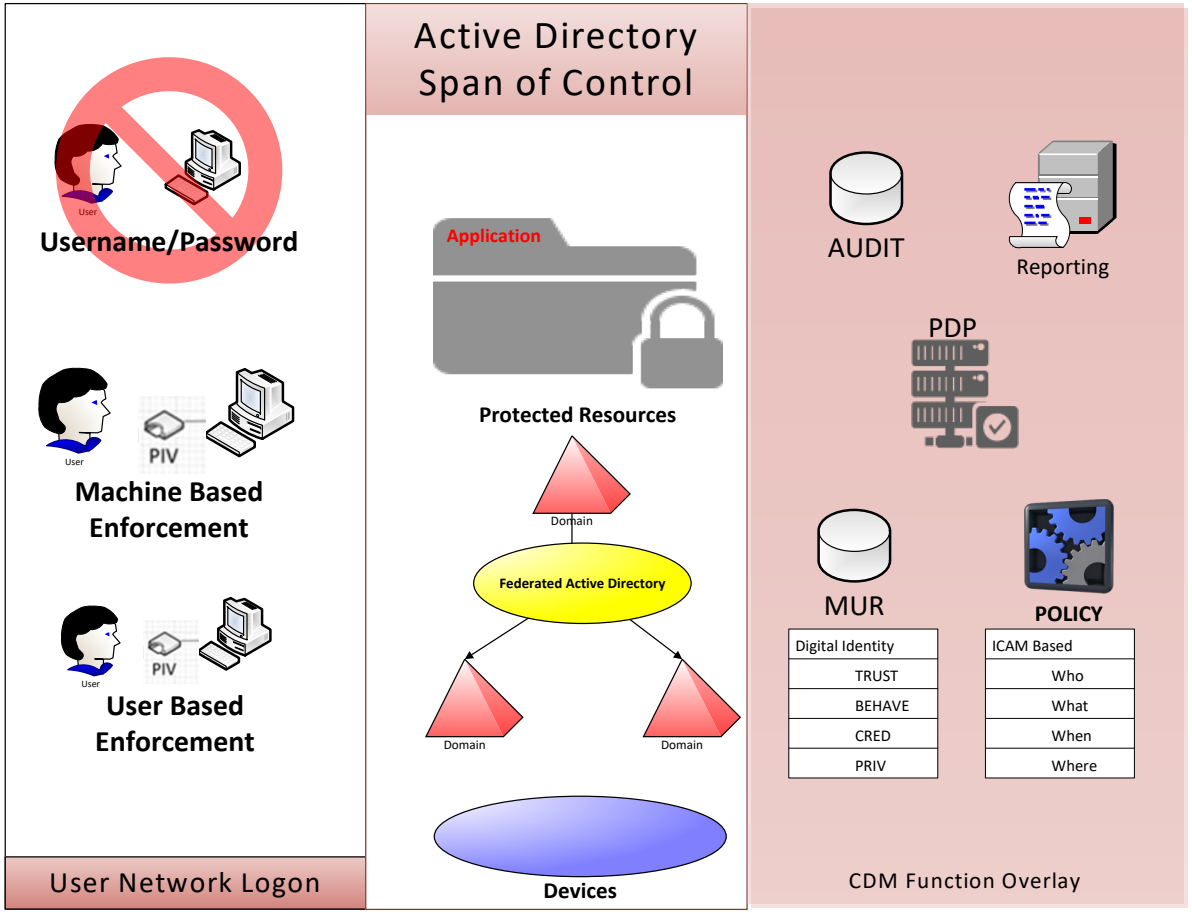
Postcondition: Individual is successfully or unsuccessfully authenticated. If successful, authorization is the next step.

CREDMGMT Use Case

- Responses from the majority of federal agencies indicated the primary control mechanism for network authentication was Microsoft Active Directory (MSAD).
- The “Authenticate a User” use case was limited to solutions that support MSAD as the primary source of account and identity information for network logon.
- CDM capabilities will overlay the agency MSAD ecosystem and move from weak to strong authentication using the PIV card.

CDM

Use Case Key Takeaways



- The MUR has all the CDM Phase 2 required data elements for metrics
- Provides visibility to the Identity Stores (e.g., Active Directory) within Enterprise
- Focus is network login with PIV card

NIST SP 800-53 Control Support

CREDMGMT provides visibility and accountability.

Policies determine which users can access which systems. That information is available in the MUR.

CREDMGMT supports the following 800-53 controls:

- Personal Security (PS) Suitability as related to TRUST
- Cyber Security Awareness Training (AT) as related to BEHAVE
- Access Control (AC), and Identification and Authentication (IA) as related to CRED

Agency Role

- CDM Phase 2 relies on existing agency policies to function.
- Agencies will need to be **more engaged** and provide Agency polices governing their users and appropriate accesses to the CMaaS integrator.
- The tools, process, and reporting of Phase 2 will not be effective if the agency has not documented and practiced ICAM policies using a **least privileges model**.
- CDM points of contact (POCs) need to **engage** the agency's ICAM office often to determine and finalize these policies so they can be reflected in the CDM tools.

People: IT Executive/Management

Program Sponsorship and Announcements

- Document and communicate commitment
  - Document the working relationship with existing CDM TO2 activities
  - Consider creating an Integrated Project Team (IPT) to include key stakeholders
  - Charter the CREDMGMT effort internally
- Communicate and foster awareness
  - Foster adoption of the ICAM and CDM programs via proactive communication and awareness

People: IT Organization & Staff Planning

Personnel Site/System Access

- Contractor will carry DHS suitability
- Reciprocity will facilitate access and logistics for contractors
  - Logical/physical
  - Prepare for agency-specific security considerations
    - Identify key stakeholders
    - Coordinate with Security Operations
- Agencies should evaluate existing resource availability to assist with implementation activities
- CREDMGMT is a turnkey solution—the agency will be responsible for operations and maintenance

Process: Program/Project Management

- Awareness and preparation to work through change management process
  - Realistic timelines and approval durations
  - Required documentation
- Logistics
  - License Transfer Process is same as TO2 process
  - Property accountability and financial implications
  - Transfer to operations support
- IT governance
  - Existing governance processes
  - Authority to Operate (ATO) process
- IT service management
  - Existing service contracts

Technology: Existing ICAM Infrastructure

- Be prepared to update Attachment G during as-is validation
- Update CREDMGMT documentation
  - Current architecture, deployments, and versions
  - Current operational status
    - New implementations, changes in infrastructure configurations, etc.
- Plan for installation
  - Ping, power, and pipe
  - Existing bandwidth limitations
- Be prepared to provide hardware and/or virtual machines to support the CREDMGMT solution

CREDMGMT Key Takeaways

- Phase 1 was about devices; Phase 2 is about people.
- CREDMGMT TO Provides Chief Financial Officers (CFO) Act agencies with ability to centrally manage credential data for general user populations:
  - Provides strong authentication and support for building the MUR
- Period of Performance (PoP) is two years; we're already almost through the first year.
- Integrator will provide design, documentation, training resources, and agency implementation support.
- MUR functional description helps vendors (KCG, CGI, Mantech) ensure common data model across Task Orders:
  - SailPoint tool will be used to create the MUR

Audience Q&A

Please use the question box on the top right of your screen to ask questions.

Get Involved with the CDM Learning Program!

Visit our website:
https://www.us-cert.gov/cdm

Engage with our weekly Insights:
https://www.govloop.com/groups/cdm-learning-bits-bytes

Join our mailing list:
cdmlearning@hq.dhs.gov

Thank you for attending today's CDM webinar!

- A certificate of attendance will be available to download at www.us-cert.gov/cdm/training within one week of today's event.
- Please help us provide better learning content by completing the short survey. Your feedback matters!