Document	
Title:	Identity, Credential, and Access Management: An interoperability capability maturity model
Publication Date:	March 30, 2015
Archive Date:	N/A
Notes:	This sample maturity model was developed by the Program Office for Information Sharing Environments (PM-ISE) in 2015. This maturity model is a sample only. If used as a sample, please update for your mission or community to address modernized policies, standards, technologies and approaches. Maturity models like this can be used to help inform activities and priorities for ICAM initiatives; develop metrics for programs; and communicate current state and target state optimizations for enterprise policies, governance and operations.

Superseding Document	
Title:	None
Publication Date:	None
URL:	None

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT AN INTEROPERABILITY CAPABILITY MATURITY MODEL

Note: items inherit from earlier maturity levels if not addressed

		LEVEL 1 – AD HOC	LEVEL 2 – REPEATABLE	LEVEL 3 – ENHANCED	LEVEL 4 – MANAGED	LEVEL 5 – OPTIMIZED
IDENTITY MANAGEMENT	Capability & Scope	• Identity as a concept does not exist separate from the credential • The credential is the identity, without additional information	• Identity as a separate concept emerges but is local to each entity (e.g., system, network, facility, door) • Individuals must establish identities at each entity separately • Structure and elements of identity vary by entity, fostering inconsistencies and duplication in identity across entities • Individuals responsible for separately notifying each entity of changes, further exacerbating inconsistencies	• Single organization-wide identity that is consumed by entities across the organization, reducing or eliminating local identities and the associated inconsistencies • Single point of service (helpdesk) for establishing and updating identities • Identity management capability partially integrated with other ICAM capabilities, but many lifecycle events processed manually	• Organization-wide identity converged with interoperable standards • Single point of self-service for appropriate identity information to reduce help desk calls • Identity management capability fully integrated with other ICAM capabilities • Identity lifecycle events are automatically pushed to appropriate consumers	• Identities originating outside the organization are accepted • Identities originating within the organization are passed to external partners • Internal and external identities are exchanged in an interoperable format and are either natively equivalent or can be mapped • Trust between organizations established via manual or automated means • Identity is continuously evaluated to ensure suitability is maintained
	Policy, Governance, & Documentation	• No formal identity lifecycle policy, either at the entity or organization level • No formal governance structure, or governance structure exists but is not empowered • Little to no identity documentation exists, or exists but is inaccurate • No documented process for identity lifecycle operations (establishing, updating, or terminating identities), or documented process not adhered to	• Formal entity-specific identity lifecycle policy • Formal governance structure exists and is empowered to manage change within the entity • Documentation exists and is accurately maintained • Documented process for identity lifecycle operations varies by entity but is adhered to	• Formal organization-wide identity lifecycle policy • Formal governance structure exists and is empowered to manage change to identity, including structure, elements, and process organization-wide • Documentation on the organization-wide implementation exists, is accurately maintained, and is available for entities wishing to consume the identity • Documented organization-wide process for managing identity, including all identity lifecycle operations, is adhered to	• Organization-wide identity lifecycle policy converged with interoperable standards • Exceptions to documented processes are recorded and reviewed periodically	
CREDENTIAL MANAGEMENT	Capability & Scope	• Entities within an organization each require and issue their own credential, often implemented differently • Credential lifecycle operations (e.g., issuance, reset, revocation) require contacting each credential issuer • Fully manual lifecycle operations • Single factor credential	• Entities within the organization each require their own credential, conforming to an organization-wide standard	• Single organization-wide credential consumed by entities across the organization (either via direct authentication or single sign on) • Central point of service for credential lifecycle operations • Partially automated credential lifecycle operations • Strong, tamper-resistant credential • Credential supports (not necessarily requires) two or more factors	• Credential system periodically verifies identity's continued eligibility for credential • Organization-wide credential converted with interoperable standards	• Automated acceptance of external credentials issued by trusted partners • Fully automated lifecycle operations
	Policy, Governance, & Documentation	• No formal credential lifecycle policy, either at the entity or organization level • No formal governance structure, or governance structure exists but is not empowered • Little to no documentation exists, or exists but is inaccurate • No documented process, or documented process not adhered to	• Formal entity-specific credential lifecycle policy • Formal governance structure exists and is empowered to manage change within the entity • Documentation exists and is accurately maintained • Documented process varies by entity but is adhered to	• Formal organization-wide credential lifecycle policy • Formal governance structure exists and is empowered to manage change organization-wide • Documentation on the organization-wide implementation exists, is accurately maintained, and is available for entities wishing to consume the credential • Documented organization-wide process for managing credentials, including all credential lifecycle operations, is adhered to	• Organization-wide credential lifecycle policy converged with interoperable standards • Exceptions to documented processes are recorded and reviewed periodically	

		LEVEL 1 – AD HOC	LEVEL 2 – REPEATABLE	LEVEL 3 – ENHANCED	LEVEL 4 – MANAGED	LEVEL 5 – OPTIMIZED
PHYSICAL ACCESS MANAGEMENT (PACS)	Capability & Scope	• Door- or area-specific PACS, each managed independently • Credential-less PACS operation (e.g., key or cypher locks), preventing the association of a specific identity with the access request • Access control decision made without identity information • No reporting or auditing	• PACS managed at the facility level, either as a single comprehensive PACS or collection of independent-yet-centrally-managed PACSs • PACS use a locally-unique credential, associating an identity with the access request • Single factor authentication or better • Access control decision made using only an identifier, without additional identity information • Access control decision based on identifier's presence on a list • Reporting and audit records captured at local PACS	• PACS across the organization accept a common credential, subject to local facility provisioning • PACS verify the presented credential's continued trustworthiness at each use • Access control decision made using only the identity information available on the credential • Access control decision based on identifier and other credential-based information • Reporting and audit records from across the organization integrated into a unified view	• PACS across the organization accept a common credential, without local facility provisioning • Multi factor authentication used where risk level indicates • Access control decision made using identity information retrieved from organization's identity management capability • Access control decision made based on roles (vs. individual presence on a list)	• PACS accept credentials issued by trusted external federation partners • Access control decision made using identity information retrieved from federation partners • Access control decision made based on identity information (vs. individual presence on a list) • Reporting and audit records returned to appropriate external trusted partner
	Policy, Governance, & Documents	• Policy, either formal or informal, established at the door or area level • No formal governance structure, or governance structure exists but is not empowered • Little to no documentation exists, or exists but is inaccurate • No documented process, or documented process not adhered to	• Formal facility-wide policies • Formal governance structure exists and is empowered to manage change facility-wide • Documentation exists and is accurately maintained • Documented process exists and varies by facility but is adhered to	• Formal organization-wide policies • Formal governance structure exists and is empowered to manage change organization-wide • Documentation on the organization-wide implementation exists and is accurately maintained • Documented organization-wide process exists and is adhered to	• Organization-wide access control policy converged with interoperable standards • Exceptions to documented processes are recorded and reviewed periodically	
LOGICAL ACCESS MANAGEMENT (LACS)	Capability & Scope	• Entities use a locally-unique credential, single factor or better • Access control decision made using only an identifier, without the benefit of additional identity information • Access control decision based on identifier's presence on a list • Reporting and audit records captured at the local entity • Access control components (policy administration, decision, enforcement, and information) woven into entity • Access must be requested in advance of need • Network or System level access control granularity	• Entities across the organization accept a common credential, subject to local provisioning • Entities verify the presented credential's continued trustworthiness at each use • Access control decision made using identity information maintained locally by the entity • Access control decision based on requestor's membership in a group or possession of a role • Access control components local to entity, but exist as discrete, identifiable components with well-documented interfaces • Collection level access control granularity	• Access control decision made using identity information retrieved from organization's identity management capability • Policy decision and enforcement components local to the entity • Access requests adjudicated real-time and on demand • Reporting and audit records from across the organization integrated into a unified view • Record/document level access control granularity	• Access control decision based on machine-readable policies that take into account information about the requestor's identity, the resource, and the context of the request • Policy decision, administration, and information components centralized across the organization • Policy enforcement component remains local to the entity	• Entities accept credentials issued by trusted external federation partners • Access control decision made using identity information retrieved from federation partners • Reporting and audit records returned to appropriate external trusted partner • Cell/field level access control granularity
	Policy, Governance, & Documentation	• Entity-specific access control policies, either formal or informal, do not necessarily align with underlying governing documents • Access requests are adjudicated manually, and without uniformity • No formal governance structure, or governance structure exists but is not empowered • Little to no documentation exists, or documentation exists but is inaccurate • No documented process, or documented process not adhered to	• Entity-specific access control policies are formally documented, but do not necessarily align with underlying governing documents • Access requests are adjudicated manually and uniformly by adhering to policies • Entity-specific formal governance structure exists and is empowered to manage change • Entity-specific documentation exists and is accurately maintained • Entity-specific documented process exists and is adhered to	• Organization-wide access control policies are formally documented and align with underlying governing documents. • Policies harmonized across entities via central policy administration and/or equivalent local entity policies • Formal governance structure exists and is empowered to manage change organization-wide • Documentation on the organization-wide implementation exists and is accurately maintained • Documented organization-wide process exists and is adhered to	• Exceptions to documented processes are recorded and reviewed periodically	