manageID
ICAM SOLUTION

ICAM on Cloud

manageID® is the complete identity, access management, and governance solution which securely manages digital identities, credentials, and access entitlements associated with the identity. This solution delivers an end-to-end lifecycle management capability.

manageID® enables secure, authenticated, and authorized access to information resources and physical assets, all from an integrated service that is easy to provision and manage.

www.citi-us.com/identity-management

IDENTITY MANAGEMENT

manageID® provides comprehensive identity management capabilities for your organization's ICAM requirements.

IDENTITY PROVISIONING

Our solution delivers flexibility of multiple methods for identity creation, with built-in support for HR-driven, sponsor-initiated, self-service, API, and digital identity. Our solution supports identity creation methods for an organization and provisioning of identities within downstream systems.

IDENTITY ASSURANCE

The solution supports NIST 800-63A Identity Assurance Levels (IAL) 1 - 3 and meets assurance requirements for various types of identities. It allows for the capture/collection of demographic and biometric identity attributes to support any organization specific business requirements.

STANDARD CONNECTORS

Leverage identity data and attributes from any data source such as HR (PeopleSoft, Workday etc.), Active Directory/ LDAP, SQL, etc. with built-in interfaces. Leverage built-in APIs for any custom integration with data sources. Concurrently connect with multiple data sources to meet organizational integration requirements.

IDENTITY DATA MANAGEMENT

Connect with multiple data sources and downstream systems and update identity data attributes based on organization specific configurations. Promote the solution to become the authoritative data source for defined attributes and support identity data de-duplication/reconciliation based on pre-defined sets of attributes.

RULES ENGINE

Automate the identity and lifecycle management processes via business rules that can be configured to meet organization specific requirement for automation. Rules are configured by business domain users and does not require any custom development and scripting support from technical staff.

COLLABORATIVE WORKFLOW

Leverage built-in workflow capability and templates to quickly configure support for any identity management related business processes. Support workflows for various types of identity (constituents) managed within the solution.

CREDENTIAL MANAGEMENT

manageID® supports creation and lifecycle management of credentials assigned to a digital identity. Each identity can be assigned multiple credentials based on the needs of the organization.

USER ID / PASSWORD

Create and manage user ID/password-based credentials in Active Directory and other LDAP compliant directories and enforce password policies for an organization.

DIGITAL CERTIFICATES / PIV-C

Our solution supports encoding and issuance of PKI technology-based credentials such as PIV-C tokens, as well as user and device certificates. Connect with industry leading PKI platforms and services via vendor-approved built-in connectors.

THIRD-PARTY AUTHENTICATION SERVICE

Use the built-in connectors with several third-party authentication products and services to provision and manage credentials within the application. The solution can co-exist with existing products and services that may be in use within an organization.

HARDWARE TOKENS

manageID® has built-in support for various manufacturers of hardware tokens that offer OTP /Oauth functionality. Our solution includes comprehensive capability to manage token stock and enables/revokes usability, based on assignment to users and lifecycle state.

PHYSICAL ACCESS CONTROL CARDS

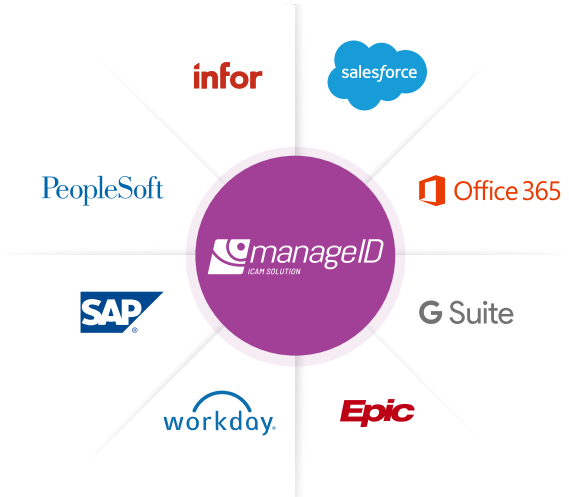
Integrate with leading Physical Access Control Systems (PACS) to provision identity and enable access via assignment of access levels. Automate the initial provisioning and lifecycle management of the PACS credential. Support various data formats for PACS credentials such as Proximity, DESFire EV1, EV2, and SEOS etc.

MOBILE / DERIVED CREDENTIALS

Our solution offers issuance and management of PKI technology based strong credentials derived on mobile devices associated with users. The derived credentials can be used to authenticate and allow access to information assets. The credentials can be derived onto non-mobile devices such as TPM chips on windows machines.

ACCESS MANAGEMENT

Manage access to all organizational information resources and physical assets via built-in access entitlement management capabilities. An organization can manage any number of external relying applications and physical access systems to control access for various types of users.



- Support NIST 800-63B-based Authentication Assurance Levels (AAL) 1-3.
- Leverage our solution to configure and enforce organizational access policies.
- Manage multiple external relying systems for enabling access entitlements. Built-in connectors for several relying systems for access assignment updates.
- Includes workflow for access request and approval with configurable levels of automation based on organization specific needs.
- Automate account and access provisioning in downstream systems and services.
- Enable authentication and authorization services via built-in MFA/SSO component, or integration with existing product and services. Support NIST 800-63B based Authentication Assurance Levels (AAL) 1-3.

LIFECYCLE MANAGEMENT

manageID® includes functionality to control the entire lifecycle for an identity, as it progresses from establishing the identity all the way to termination and archival of the identity record. During this process it also supports the lifecycle stages of "credentials" and "access" associated with an identity. Overall the solution orchestrates the relationships between the identity, and all linked credentials and access.

- Policy based lifecycle actions for identity, credential, and access attribute updates.
- Solution provides a person centric view of the digital identity, credentials and access entitlements.
- Self-service, helpdesk, and admin functionality for lifecycle management of identity, credentials, and access.

GOVERNANCE

manageID® includes built-in functionality to be leveraged as an effective tool to configure and implement identity and access governance processes. The configuration and transactional audit data regarding identity access entitlements and relying systems is leveraged for this purpose.

- Configure business process for access attestation/ certification in support of organizational risk.
- Create and deliver person, application (software or hardware relying system), or (sub)-organization-based attestation reports.
- Automate access lifecycle updates based on business rules configured for organization.

KEY BENEFITS

manageID® ICAM provides a collection of business, functional, technical, and security benefits for any organization, bred from CITI's comprehensive business practices based in identity, credential, and access activities over the past 15 years. The modular architecture and high level of configuration makes the manageID® solution ideal for any organization. The benefits listed are common amongst all organizations that have chosen to use manageID® to revamp their ICAM implementation.

ENHANCED USER EXPERIENCE

The manageID® solution provides an enhanced user experience which allows the user to:

- Access to a self-service portal for users to reset passwords, change security questions, recover accounts, and request further access.
- Configurable login pages per organization unit to minimize impact on user experience.
- View a custom user dashboard to access applications and resources based on organizational assignments.

ENHANCED ADMIN CAPABILITY

The manageID® solution enables system administrators to meet organizational needs for solution management and access control:

- Access to built-in integrations with external systems via UI-based configuration, minimizing expensive customizations.
- Provide comprehensive and granular access control (via user/role management) and flexible authentication options.
- Control permissions to identity/access data based on organizational security policies.
- Enable de-centralized access approval processes customized for specific organizational hierarchies.
- Configure organizational structure based workflows for identity onboarding and access control.
- Perform all configurations via a web-based interface, making custom code and scripting seen in legacy IAM systems completely unnecessary.
- Configure multiple custom login pages based on the organization's needs.
- Configure custom user dashboards to access applications and resources based on the organization's needs.

ENHANCED SECURITY POSTURE

The manageID® solution helps organizations enhance their information security management and business risk posture. Features that deliver a high level of security assurance include:

- Create and enable the use of strong (PKI) credentials for user authentication.
- Provide authorized users with a comprehensive auditing platform for reporting and analysis.
- Real-time visibility into organizational access entitlement including lifecycle updates.
- Minimize risk associated with manual enforcement of policies related to account and access provisioning/de-provisioning.
- Support for regulatory compliance and industry vertical specific security requirements.
- Complies with NIST security guidelines, ISO 20000 and ISO 27000 based processes and procedures for a high level of security assurance.

BUSINESS BENEFITS

The manageID® solution from the offset offers several business benefits which include:

- Offload identity, credential, and access management to experts to focus on core business capabilities, transferring business and security risk.
- Minimal startup costs and subscription-based modular pricing per functionality.
- Reduce manpower requirements to provision and support identity, credential, and access management capabilites.
- Adapt to changing business and regulatory environments, e.g. acquisitions, change in regulations, etc.
- Support business initiatives to modernize IT and adopt cloud services.
- Minimize rip and replace methodology and gradually migrate to this solution.

manageID ICAM SOLUTION

CITI CREATIVE INFORMATION TECHNOLOGY, INC.

7799 Leesburg Pike, Suite 500 North
Falls Church, VA 22043

(703) 483-4300
www.citi-us.com | info@citi-us.com

About CITI: Established in 1996, Creative Information Technology, Inc. (CITI) is headquartered in Falls Church, Virginia, and have offices located throughout the United States, Europe, South Asia, and Canada. CITI is a diverse organization filled with talented IT and certified business professionals. We are certified in ISO 9001:2015, ISO 20000-1:2011, ISO 27001:2013, CMMI DEV Level 3 for Services, and CMMI-DEV Level 5 for Development. As a Microsoft Gold Partner, we specialize in the creative use of agile methods and emerging technologies.