OXFORD COMPUTER GROUP

OCG US - A MajorKey Technologies Company

MajorKey

# NomadID

## Mission-Ready Identity Management for Federal Agencies in DDIL Scenarios

# Table of Contents



SUMMARY

The DOD operates in environments with limited connectivity, necessitating an ICAM solution for access to critical systems. While existing solutions offer some capabilities, they do not currently fulfill all DDIL requirements. This document presents NomadID, a DDIL ICAM solution that integrates various components to provide the necessary capabilities to support the DOD's DDIL requirements.

NomadID includes components for identity management, security monitoring, and identity governance, with a primary identity source and provisioning mechanisms for authentication and SSO for applications and services at the edge. The identity services are co-located with authentication components to provide identity management and governance in both connected and disconnected operations.

NomadID provides a highly mobile, compact package that can be quickly deployed and utilized in a variety of tactical and edge environments.

INTRODUCTION

# A DDIL ICAM Solution For Edge Environments

The Department of Defense (DOD) has multiple requirements to operate in Disconnected, Denied, Intermittent, and/or Limited Bandwidth (DDIL) environments. DOD units may deliberately choose to operate in these environments, but they also operate in these environments due to equipment failure or outages, or they are forced to operate in these environments due to hostile action.

While connected to the enterprise network, DOD organizations have access to the full capabilities of cloud services. When operating in a DDIL environment, DOD units must retain access to mission-critical systems to conduct assigned missions. A key capability necessary to retain access to mission-critical systems is an Identity, Credentialing, and Access Management (ICAM) solution that enables DOD organizations to maintain access to critical systems.

## ICAM and Zero Trust

Existing ICAM solutions allow customers to deploy and achieve a Zero Trust Architecture (ZTA) by providing advanced security and access controls, core directory services, advanced identity protection, and application access management. The patterns in the existing solution and those in the proposed solution are replicable and extensible, such that the solution pattern could be leveraged to provide services for a variety of networks and use cases.

## Path Redundancy

It is important to recognize that "path redundancy" is critical to extending the enterprise services as close to the tactical edge as possible. This can include satellite, 5G, local internet providers, and government-owned network paths. Path redundancy reduces the number of disconnected scenarios, provides a better user experience, and significantly increases operational visibility and cybersecurity protections.

Several DOD organizations have requested an ICAM capability that will operate in a DDIL environment. However, existing ICAM solutions do not fully support the DOD's DDIL requirements for full Disconnected Mode operations.

The purpose of this white paper is to present a DDIL ICAM solution that integrates various components to provide the necessary capabilities to support the DOD's DDIL requirements. NomadID maintains authentication (CAC enabled) and Single-Sign-On (SSO) capabilities for DOD organizations operating in a DDIL environment.

CAPABILITIES

# NomadID's Key Capabilities

| *Capability* | *Description* |
|---|---|
| **Cyber Hyper Scaler Integration** | • Leverage any cloud IDP for the primary source of identities to synchronize identities and entitlements specific to a unit and applications. |
| **DDIL Cutover** | • Enable the migration of ICAM services from the enterprise environment to the DDIL environment in either a manual or automated failover fashion.<br>• Enable the migration of ICAM services from the DDIL environment back to the enterprise environment in either a manual or automated failback fashion.<br>• Provide the capability to do a security analysis of the activities and transactions conducted in the DDIL environment prior to reconnecting to the enterprise environment. |
| **Authentication** | • Enable authentication (including CAC enablement and SSO capabilities) to local applications while completely disconnected from the internet |

SOLUTION ARCHITECTURE

# NomadID's Four Environments

**Environment A** represents the home station environment where ICAM services include authentication and SSO. This environment contains a full range of cloud services, applications, and other services to support a full enterprise environment. For the purposes of capability, we will focus on the ICAM capabilities relevant to supporting a DDIL environment.

**Environment B** serves as a demilitarized zone providing a temporary environment where logs and transactions can be stored and analyzed. The DDIL environment will not be re-connected to the home station (Environment A) until all logs and transactions are analyzed and the determination is made that reconnecting the environments does not pose a threat to Environment A.

**Environment C** is a stack device that will provide temporary ICAM capabilities while in a DDIL mode of operation. These capabilities focus on providing authentication and SSO capabilities for local applications that are still available when disconnected from the internet.

**Environment D** is a stack device simulating two local applications that are still available to the DDIL network.

## Environment A: Primary Identity Management Service

The primary identity management service provides core directory services, advanced identity protection, and application management to deliver SSO access to on-premises and cloud-based applications. This allows users in different types of access scenarios to stay connected and productive.

The service provides a full range of modern identity and access management capabilities, including conditional access with multi-factor authentication (MFA) and password-less login options, SSO, self-service password management, and role-based access control (RBAC). Its intelligent security monitoring and alerting capabilities are already integrated with the DOD security monitoring and response capabilities.

In this environment, an orchestrator monitors the availability of the primary identity service at runtime. Should it be unavailable for any reason, authentication requests are automatically routed to an alternative service to support in-theater DDIL situations as they arise.

## Environment B: Security Information and Event Management (SIEM) Solution

The SIEM solution is a cloud-native service enriched by AI and threat intelligence, delivering end-to-end protection across multi-cloud and multiplatform digital estates. With innovations focused on SOC productivity, efficient threat investigations, and cost optimizations, the SIEM empowers defenders to stay ahead of threats in a simplified, scalable, and accelerated manner.

### *Generative AI-Powered Security Solution*

NomadID increases the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale. It provides a natural language assistive experience that supports security professionals in incident response, threat hunting, intelligence gathering, and posture management scenarios.

## Environment C: Enteprise Identity and Governance Platform

The identity and governance platform provides a single pane of glass into a user's access across enterprise data, infrastructure, and applications both in the cloud and on-premises. This platform combines intelligent governance processes with usage and risk analytics that are already in use within DOD agencies.

The platform is critical in managing access and entitlements in a disconnected (DDIL) state. It provides tools and features needed to manage identities, access, and compliance across both enterprise and tactical DOD environments, including functioning in a disconnected environment.

An orchestrator's role in this environment is to automatically route authentication requests to an alternative service when the network is unavailable in DDIL operations.

Key components of the enterprise identity and governance platform include:

- ***Identity Management***: Manages and provisions user identities and attributes across systems, applications, and networks.
- ***Access Management***: Controls access to resources based on user roles, policies, and compliance requirements.
- ***Analytics and Reporting***: Offers real-time dashboards, customizable reports, and historical data analysis to gain insights into deployed environments.
- ***Auditing & Alerting***: Tracks user activity, changes to policies and settings, and access to resources.
- ***Connectors***: The platform provides connectors for various cloud-based and traditional enterprise platforms, enabling interaction with resources within a variety of cloud and on-premises environments.
- ***Credential Management***: Allows administrators to securely manage and distribute user credentials across their IT environment.
- ***Self-Service***: Provides portals and workflows to enable users to perform certain tasks, such as resetting passwords, requesting access to resources, or starting onboarding or offboarding workflows.

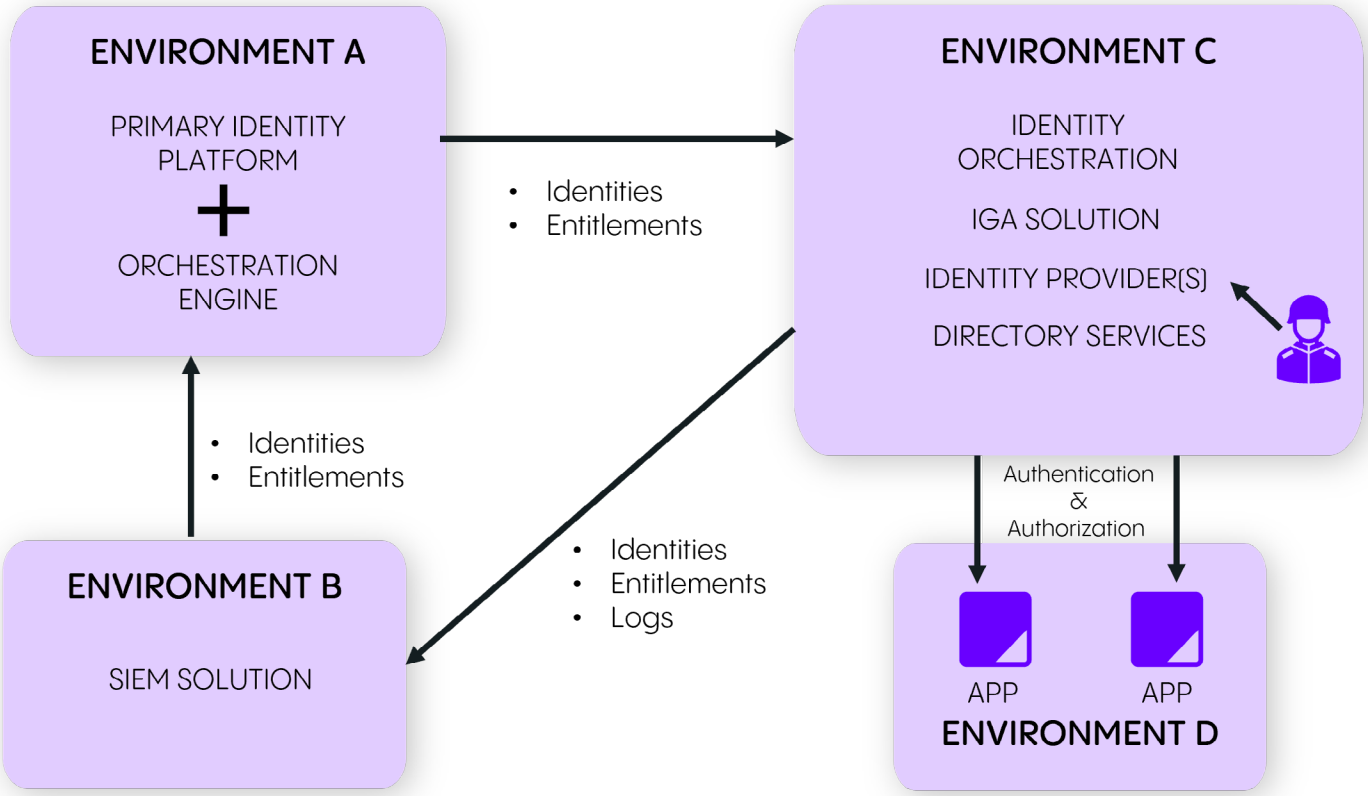


Figure 1: NomadID Identity Architecture Overview

TECHNICAL APPROACH

# NomadID's Overall Technical Design

NomadID takes identities from the primary identity service in Environment A and provisions them to the identity and governance platform in Environment C. The integration includes a mechanism that routes authentication requests to the appropriate identity provider (IDP) based on health check availability and/or manual decisions made to operate in Disconnected Mode during DDIL operations. This integration occurs in real-time or as needed, depending on the use case.

The identity and governance platform provides identity services and provisions users into an authentication service, allowing it to be utilized for authentication and SSO at the edge to support applications and services. An orchestration layer provides capabilities that intelligently route user authentication requests to either the primary identity service or the alternative authentication service based on mission parameters and network availability. The identity and governance platform is co-located with the authentication service to provide identity management and governance in both connected and disconnected operations. These components are deployed into a containerized stack environment.

NomadID offers a highly mobile, compact package that can be quickly deployed in a variety of tactical and edge environments.

TECHNICAL COMPONENTS AND CONFIGURATION

# Identity Components

## Identity Provisioning

In order to populate identities from the primary identity service in Environment A to the identity and governance platform in Environment C, NomadID utilizes System for Cross-Domain Identity Management (SCIM) provisioning through an open standard protocol for automating the exchange of user identity information between identity domains and IT systems. This protocol is already in use by the DOD for provisioning identities from their primary identity service to other cloud service providers.

To configure SCIM provisioning to the identity and governance platform, app setup is straightforward and can be integrated accordingly. This allows NomadID to synchronize any identity from the primary identity service to the alternative authentication service via the governance platform for use in authentication and authorization of users to services at the edge.

During DDIL operations, administrators can still provision users directly to the governance platform via the admin console and utilize the IDP capabilities of the alternative authentication service. The co-location of the governance platform with the IDP allows for the use of automated workflows to facilitate onboarding, offboarding, and other entitlement actions while disconnected.

These capabilities enable enterprise ICAM services at the edge where traditionally large infrastructure builds were required to provide similar services.

Automating the creation, maintenance, and removal of user accounts across various systems and applications in this lightweight model provides flexibility in several scenarios, from base/post continuity to small tactical operations.

## Identity Provider Services

### *Authentication*

The main authentication and authorization (AA) provider for NomadID is a full-featured IDP that supports multiple authentication types built out in authentication flows.

Authentication types include passwords, smart cards, FIDO2 security tokens, and one-time passcodes (OTP). These methods support the configuration of phishing-resistant MFA and CAC authentication with smart card flows.

The IDP provides SSO for applications and services that support modern authentication protocols, including OpenID Connect (OIDC), OAuth 2.0, and SAML 2.0. It can also integrate with existing LDAP and Active Directory domains, allowing the use of legacy protocols like Kerberos.

Realms within the IDP are used to manage objects such as users, applications, roles, and groups, with users belonging to and logging into specific realms. Realms can be configured to support various tactical scenarios, such as integrating with partner forces by provisioning identities directly into the IDP to support AA functions for those partners.

As part of integration with partner or third-party forces, additional authentication flows can be configured to support the authentication methods used by those partners.

The IDP supports all standard modern authentication protocols, including SAML 2.0, OAuth 2.0, and OpenID Connect. By leveraging application proxy capabilities, forces can extend support for applications using form-based, Kerberos-based, and header-based authentication.

The governance platform offers SAML-based SSO service, which can be configured to allow seamless authentication and authorization into the identity management service.

- Support authentication and authorization assertions
- Support for federal identities
- Ability to evaluate identity proofing and authentication factors

### *Authorization*

The IDP supports multiple fine-grained authorization policies and can combine various access control mechanisms, including Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), User-Based Access Control (UBAC), Context-Based Access Control (CBAC), Rule-Based Access Control, and Time-Based Access Control.

### *Orchestration*

The orchestration layer provides identity continuity that prevents application interruptions by failing over to an alternate on-premises or cloud IDP when the primary IDP goes offline. This decoupling of apps from the underlying identity logic makes it possible to implement modern authentication methods, such as passwordless authentication, and enforce consistent access policies without refactoring mission apps.

## Identity Governance

### *Privileged Access Management*

The governance platform offers features that support complete access governance for privileged, service, shared, and generic identities. It allows for managing account ownership, check-in and check-out of elevated access, time-bound access, approval processes for elevation, and logging of privileged activity. It also provides separation of duty checks based on usage and uses behavioral analytics to detect and protect against suspicious or malicious activity.

For NomadID, the governance platform integrates with the IDP via a custom API connector, enabling interaction and control over IDP resources. This integration provides privileged access management with the governance platform's advanced features.

In addition to privileged access management, the platform offers requestable and governed access to credentials, just-in-time (JIT) credential access, and session management to workloads such as Linux, Windows, and web applications. These types of access are used instead of privileged access when sessions need tight governance, monitoring, and credential reset. Combined with the IDP for SSO, CAC, or other MFA-based access, privileged workloads are securely managed.

### *User Management Workflow*

Automated workflows within the governance platform are used to manage the identity lifecycle, including the provisioning of users and entitlements for any platform with a configured connector. This capability extends to various environments, including Active Directory domains, LDAP directories, and other built-in or custom connectors provided by the governance platform. These provisioning and identity management capabilities allow for the onboarding (joiner) or offboarding (leaver) of users within the environment.

## Support Services

### *Logging and Administration*

Both the IDP and the governance platform include built-in logging capabilities. Logging can be viewed in two perspectives. First, when NomadID has connectivity back to the enterprise, whether that be a DOD tenant or another enterprise environment, both platforms are configured to push logging back to the organization's SIEM solution for monitoring and analysis by DOD personnel.

SIEM integration is crucial to the security framework of DOD agencies, feeding security information from these applications into a SIEM to monitor and manage security events across the enterprise. The IDP provides console, file, and log handlers configurable for system and server-level logging for local analysis or enterprise SIEM integration.

The governance platform offers specific components for SIEM product integration, recording all user activities in the form of security audit logs. These logs can be extracted into CSV files and transferred to cloud storage for consumption by the enterprise SIEM. Once ingested, filters can be applied to search required patterns and monitor user activity.

Enterprise SIEM integration provides the DOD Security Operations (SOC) team with visibility into events occurring in edge environments for both the IDP and governance services.

In disconnected operations, the same level of logging remains available, but monitoring and analysis would occur locally on systems, managed by security and/or ICAM administrators.

# Accredidation

NomadID would be a candidate for accreditation and Authority to Operate (ATO) approval.

Both the IDP and governance platform are already used in various programs and projects throughout the DOD. The governance platform is in use in the DOD tenant and undergoing vendor accreditation, while the IDP is deployed in multiple accredited programs within the DOD. Extensive documentation and experience with both services within the DOD will assist in navigating the ATO approval process.

# About

Oxford Computer Group, a MajorKey Technologies company, has specialized in Microsoft identity, security, and governance solutions for over two decades. We design and develop innovative solutions focused on delivering business value. We assess architectures and processes, and make recommendations designed to support strategic objectives. To accelerate deployment, we use our proven methodology, best practices, and a unique library of code developed during 900+ projects.

OCG is a member of the Microsoft Intelligence Security Association (MISA). We have won the Microsoft Partner of the Year award eight times, and were a finalist for both the Identity and Defense & Intelligence Microsoft Partner of the Year awards in 2023, 2024, and 2025.

## Thank you for reading!!

We appreciate your time and interest in exploring NomadID.

To learn more, connect with our experts, or explore additional resources, please visit us at majorkeytech.com or open the QR codes below.

NomadID web page

Request a demo