delviom
INSIGHT | ANALYTICS | SECURITY

Coalition Identity and Access Management (Co-IDAM) Cards

Interoperable Identity and Access Solutions for Multi-Jurisdictional Missions

White Paper

44790 Maynard Square, Suite 280 | Ashburn, VA 20147 | Email: Info@delviom.com

Table of Contents

Restrictions

This material is for general informational purposes only and should not be considered legal, financial, or professional advice. While efforts have been made to ensure accuracy and relevance, no representation or warranty is given as to the completeness or applicability of the information for your particular situation. Government agencies, commercial organizations, and other stakeholders should consult qualified advisors for guidance specific to your organization or circumstances.

Coalition Identity and Access Management (Co-IDAM) Cards

A White Paper on Interoperable Identity and Access Solutions for Multi-Jurisdictional Missions

Timothy Mayers Jr., CISSP, CEH, CCSK, Delviom - Chief Cyber Solutions Architect

Executive Summary

As digital transformation accelerates across governments, critical infrastructure, and international alliances, the need for secure, interoperable, and policy driven identity systems has never been greater. Organizations increasingly conduct operations through distributed teams, temporary coalitions, and cross agency collaborations, yet most identity and access management systems remain siloed, inconsistent, and difficult to scale.

The Coalition Identity and Access Management (Co-IDAM) solution developed in partnership between **Delviom** and the **Foundation for Trusted Identity (FTI),** addresses this gap by delivering a unified Identity and Access Card Management System (IACMS) designed for high assurance, multi-tenant, multi-jurisdictional environments. Co IDAM has been operational in regulated U.S. government environments since 2017 and is engineered to support organizations that must form secure, temporary, and mission specific alliances without sacrificing autonomy or governance control.

ENTERPRISE-SCALE PIV-I ISSUANCE FOR MULTI-JURISDICTIONAL MISSIONS

The Delviom/FTI Co-IDAM platform has supported large-scale PIV-I credential issuance across **45 U.S. organizations,** including multiple local agencies, **four tribal nations, and six U.S. territories,** enabling broad adoption of modernized cybersecurity and identity assurance practices. Co-IDAM also provided PIV-I credentialing services for major federal programs, including the **U.S. Department of Education, U.S. Department of Energy,** and the **Federal Emergency Management Agency (FEMA),** ensuring compliance with Homeland Security Presidential Directive 12 (HSPD-12) and advancing secure, standards-based identity management nationwide.

Introduction

Cybersecurity threats, regulatory pressure, and operational complexity continue to challenge traditional identity and access management models. Digital identity cards, mobile credentials, and high-assurance smart card systems have emerged as essential tools for reducing unauthorized access, preventing data breaches, and enabling secure remote and cross-domain operations. Yet organizations still face significant obstacles:

- Fragmented or inconsistent identity governance
- Manual onboarding and offboarding processes
- Excessive reliance on passwords and shared credentials
- Inadequate auditing, compliance reporting, and event traceability
- Difficulty supporting temporary or multi-entity mission environments
- Risks of insider threat, identity fraud, or privilege escalation

Co IDAM was developed to directly address these operational and security challenges with a scalable, standards based, coalition ready identity solution.

The Coalition Identity Challenge

Modern missions increasingly require seamless collaboration across agencies, jurisdictions, and nations, yet most identity systems are built on outdated assumptions, including a single governing authority, a permanent organizational structure, and tightly controlled network boundaries. These assumptions quickly fail in operational environments where multiple agencies must coordinate at speed, each organization must retain sovereign control over its identity authority, implicit trust cannot be granted, and identity data must remain strictly partitioned according to policy domain. As a result, organizations face:

- **Limited visibility** into user identity and access across coalition partners
- **Complex provisioning** when multiple credential types or roles are needed
- **Audit and compliance challenges** across different jurisdictions
- **Data privacy conflicts** driven by differing legal frameworks

Co-IDAM bridges these divides by providing a **federated but shared** identity card service that supports both distributed and centralized governance models.



Co-IDAM Overview

The Coalition Identity and Access Management solution is built around a comprehensive **Identity and Access Card Management System (IACMS)** engineered for coalition operations. Key functional components as depicted in the graphic below include Identity Lifecycle Management, Smart Card and Credential Issuance, PKI and Trust Framework Integration, Workflow and Approval Orchestration, Audit and Compliance Logging and Integration with Logical and Physical Access Systems:

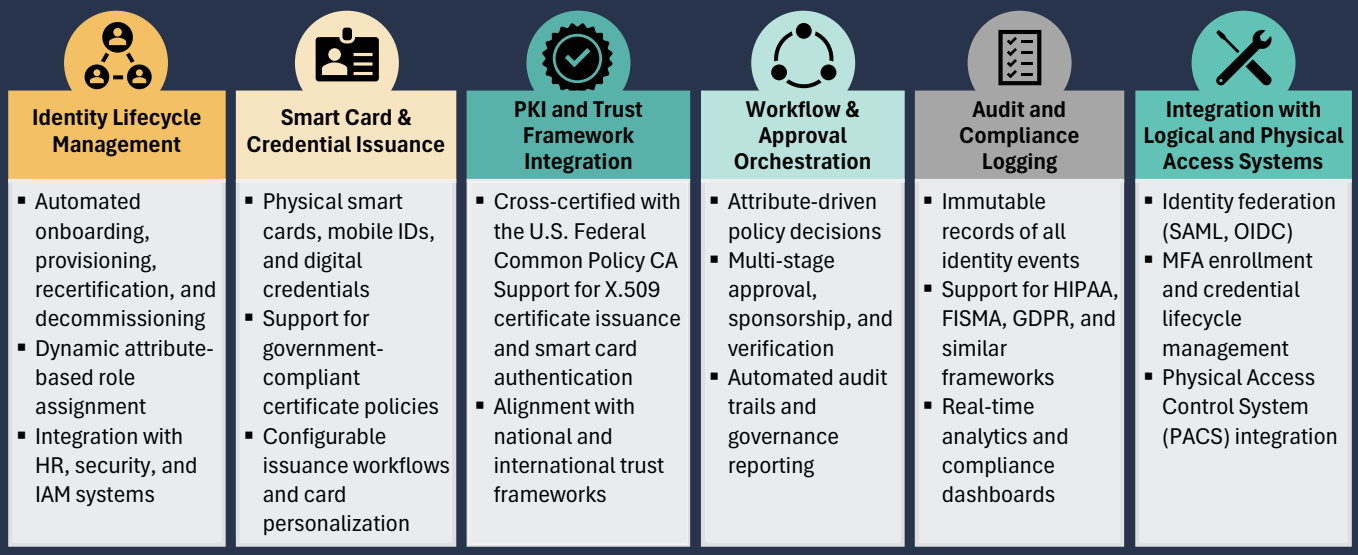

Figure 1: Delviom's IACMS for Coalition Operations

Coalition-Centric Design

Co-IDAM is **purpose-built for environments that require interoperability without forced trust consolidation, enabling organizations to collaborate securely while retaining full governance autonomy.** The platform supports multiple certificate profiles, multiple governance authorities, policy-partitioned domains, and entity-specific configuration and workflow logic, ensuring each participant can apply its own rules and credentialing standards. Credential assurance is maintained through high-assurance identity proofing, robust PKI integration, attribute and policy enforcement, and standards-based authentication mechanisms. Together, these capabilities allow coalition partners to operate securely, independently, and efficiently within a shared identity ecosystem.

Badge and Credential Customization

Co-IDAM supports highly flexible badge design and data-driven card generation, enabling organizations to manage multiple templates aligned with specific roles, units, or operational needs. The platform allows full configurability of text, logos, images, barcodes, and QR codes, along with conditional display of fields based on user attributes to ensure accurate representation of identity data. It supports both PDF credential generation and physical card printing, while maintaining full compatibility with ISO/IEC smart card standards. **All badge layout elements are tightly bound to authoritative identity records, ensuring consistency, auditability, and trust across the credentialing process.**

Operational Model

The Co-IDAM platform operates as a secure, fully managed service within a virtualized infrastructure, delivering a stable and scalable foundation for coalition identity management. Its architecture is built on a single monolithic codebase to ensure consistency and uniform functionality across all deployments, while supporting multi-tenant operations with strict tenant isolation to protect organizational boundaries and sensitive data. Although standardized features are available to all clients, the platform also enables entity-specific policies and configurations, allowing each organization to tailor workflows and governance controls to its unique requirements. **This unified design simplifies patching, upgrades, and overall lifecycle management, reducing maintenance complexity and operational burden.** As a result, the model lowers total overhead while strengthening security posture and promoting governance uniformity across all coalition members.

How We're Different

Delviom's Co-IDAM solution differs fundamentally from traditional commercial IDAM platforms by being purpose-built for high-assurance, coalition, and multi-jurisdictional environments, rather than single-enterprise use cases. While most commercial IDAM vendors assume a single governing authority, unified trust domain, and static organizational structure, **Co-IDAM is architected to support sovereign identity ownership, policy-partitioned domains, and federated governance without forced trust consolidation**. It integrates high-assurance smart credentials, PKI cross-certified with U.S. Federal trust frameworks, and tightly coupled physical and logical access controls, capabilities often treated as add-ons by commercial vendors. Proven in regulated government environments since 2017, **Co-IDAM emphasizes auditability, interoperability, and standards-based assurance over proprietary lock-in**, enabling temporary alliances, mission partners, and coalition members **to operate securely and autonomously** within a shared identity ecosystem.

Benefits and Value

Co-IDAM delivers measurable advantages across mission, security, and operational dimensions:

Mission and Operational Benefits

- Supports coalition and national integration models
- Enhances workforce accountability and situational awareness
- Improves emergency response through identity-linked event management
- Enables seamless onboarding/offboarding across agencies

Cybersecurity and Compliance Benefits

- Strong authentication reduces unauthorized access risk
- Cryptographic identity ensures high-assurance verification
- Comprehensive audit logging enhances governance
- Meets HIPAA, FISMA, GDPR, and similar regulatory requirements

Cost and Efficiency Benefits

- Reduces lifecycle costs across identity issuance and maintenance
- Improves provisioning accuracy and eliminates manual bottlenecks
- Minimizes system duplication using a shared but segmented platform

Enterprise and Government-Scale Maturity

- Operational in multi-jurisdictional environments since 2017
- Vendor-neutral, standards-based architecture
- Proven interoperability across diverse mission partners

Why Delviom

Delviom provides **a full range of cybersecurity services for both federal and commercial clients**, and holds multiple certifications including ISO 27001, CMMI Level 3, and DoD CMMC Level 2, reflecting our commitment to high-quality and secure service delivery. Delviom serves as the solution integrator, modernization partner, and service provider supporting Co-IDAM deployments. Delviom brings:

- Deep expertise in digital identity, PKI, and secure access
- Engineering and integration capability across both logical and physical access systems
- Rapid configuration and deployment support
- Governance, compliance, and policy alignment expertise
- Continuous innovation through agile processes and technical modernization

Delviom ensures Co-IDAM customers **benefit from a secure, scalable, and future-ready identity ecosystem** capable of supporting complex mission requirements. Delviom provides a robust, interoperable, and mission-ready framework for managing digital identities across distributed and multi-jurisdictional environments. With a proven foundation in regulated government programs and a design optimized for coalition operations, Co-IDAM equips organizations with the capabilities needed to establish trust, strengthen security, and accelerate mission outcomes in an increasingly interconnected world.

Next Steps: From Strategy to Action

Delviom stands ready to offer organizations **a clear, low-risk path from evaluation to operational deployment** of coalition-ready identity capabilities through the Co-IDAM platform. As a next step, Delviom provides a structured engagement that may include a limited-scope pilot to validate interoperability, governance, and assurance within the customer's environment, followed by a targeted identity roadmap and governance consultation to align policies, partners, and mission requirements. For organizations ready to advance, Delviom supports transition from pilot to production with integration, credential lifecycle operations, and managed services, **enabling stakeholders to move confidently from concept to sustained, multi-jurisdictional identity operations.**

Contact Us

Web: Delviom.com
Email: info@delviom.com
Phone: +1 (703) 953-2535

Web: Delviom.com
Email: info@delviom.com
Phone: +1 (703) 953 2535