



Identity Services Design Concepts

Current State

The Department of the Navy (DON) systems and networks operate using 20-year-old design patterns for identity. They are stove piped around application and network boundaries preventing network, application, and data interoperability. Current solutions only address authentication and authorization. They do not provide the type and level of control, monitoring, automation, and reporting needed to ensure security and operational flexibility in the modern hybrid operating environment. Identity is the foundation for supporting modern, secure, and interoperable hybrid cloud operations. Identity Services are of critical importance as a supporting service to all modernization efforts.

Problem Statement

The DON must aggressively adopt modern industry identity capabilities as part of Digital Enterprise Services to integrate access and authorization seamlessly across DON security and network boundaries. The DON seeks a fully integrated industry solution to modernize identity operations across hybrid multi-cloud and Denied, Disconnected, Intermittent, and Low-bandwidth (DDIL) and environments.

Identity Services Design Requirements

- Provide context aware security: identity, device, network, and resource combination
- Integrate with AI and ML to support Continuous Adaptive Risk and Trust Assessment (CARTA)
- Dynamically assign entitlements based on user role (RBAC) and/or attributes (ABAC)
- Self-Service for domain and app owners to maintain control of their identities and authorizations
- Resource owners can link entitlements to any identity from any domain
- Multiple personas can be linked and tracked to a single individual or entity
- Move to Zero-Trust security model – improve overall security
- Identity services integrate with Data Loss Prevention and security services to ensure data level security
- Identity federation and synchronization without Active Directory federation
- Resolve afloat/ashore disparity using identity information synchronization
- Design as loosely coupled services/micro-services to operate across network and security boundaries
- Expand identity services to achieve commercial identity services parity
- Federate disparate sources of identity information and aggregate them for consumption
- Enable identity services for non DoDIN-N users and Bring Your Own Device (BYOD)
- Enhance user experience through non-CAC authentication, single sign-on, and self-service
- Enable fully automated Federal Information System Controls Manual (FISCOM) compliance
- Adopt alternative multi-factor authentication approaches based on use case

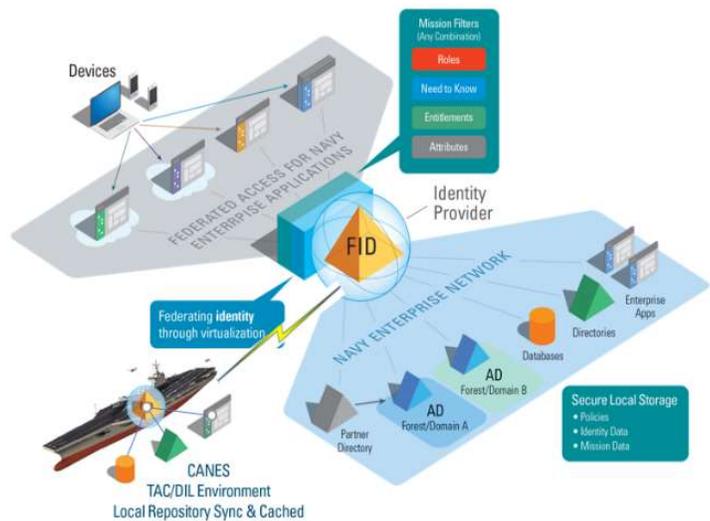


Figure 2: Identity Services OV-1

Identity Services			
Identity Federation Svcs	Access Mgmt Svcs	Identity Mgmt Svcs	Audit Role & Compliance Svcs
• Identity Data Aggregation (Meta Directory)	• Web Access Mgmt/SSO	• User Self-Service	• Centralized Audit
• Identity Data Distribution (Virtual Directory)	• Federated Identity Mgmt/SSO	• Delegated Administration	• Logging and Monitoring
• Real-time & Disconnected Ops Synchronization &	• Authentication & Authorization	• Automation Workflow Approvals	• Access Certification
• Privileged Access Management Integration	• Access Mgmt APIs	• Enterprise Role Definition	• Per-User and Per-Asset Reporting

Figure 1: Identity Services Capabilities

Chief Architect, DON CIO. April 10, 2020.

DISTRIBUTION A. Approved for public release. Distribution unlimited. (28 May 2019)