

# ICAM Engineer

## ICAM Engineer

The ICAM Engineer is responsible for implementing, configuring, and optimizing Identity, Credential, and Access Management (ICAM) integration of the Electronic Point of Sale (EPoS) system into the DLA Enterprise ICAM environment. This role focuses on hands-on deployment, integration, and sustainment of EPoS ICAM integration while ensuring compliance with DoD, DLA, and federal access control standards. The engineer works closely with architects, analysts, and program managers to deliver secure, functional, and scalable solutions aligned with Zero Trust and Agile methodologies.

### Duties and Responsibilities

- Integrate EPoS systems with DLA ICAM Okta for Single Sign-On (SSO) services and ensure interoperability with enterprise applications.
- Implement secure access controls and user provisioning workflows in line with enterprise standards.
- Support testing, troubleshooting, and resolution of ICAM-related technical issues.
- Apply DoD, DLA, FISCAM, and Zero Trust requirements to DLA ICAM system integration.
- Document system builds, configurations, and changes to ensure accurate sustainment records.
- Collaborate with architects on solution design and with testers on validation activities.
- Monitor ECOM ICAM integration performance, identify vulnerabilities, and recommend improvements.
- Support Agile delivery cycles, contributing to sprint planning, execution, and backlog refinement.
- Provide technical input for modernization and sustainment of EPoS ICAM environments.

### Required Skills and Experience

- Bachelor's degree in IT, computer science, engineering, or related field.
- 5+ years of experience implementing or managing ICAM, IAM, or enterprise security solutions.
- Strong technical expertise with authentication protocols (SAML, OAuth, OIDC), PKI, and Active Directory/LDAP.
- Hands-on experience integrating third party applications into Existing Enterprise ICAM platforms using OKTA APIs.
- Familiarity with DoD/DLA security policies, RMF, and Zero Trust frameworks.
- CompTIA Security+ or CISSP required; Microsoft, AWS, or IAM certifications preferred.
- Strong troubleshooting, documentation, and integration skills.
- Experience in Agile environments with iterative delivery.
- Active DoD security clearance (or ability to obtain).
- Must work on-site in Coggins HQ, Alexandria, VA.