Use of Service Accounts in a Zero Trust Architecture (ZTA)

1. Introduction

This guideline covers managing and using service accounts in compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture. These guidelines aim to ensure the secure use of service accounts while adhering to the core principles of least privilege, continuous monitoring, and strong authentication mechanisms. By adhering to NIST SP 800-207, we can enhance service account security, enforce strict access controls, and align with Zero Trust principles.

2. Scope

This guidance applies to service accounts used in:

- **API Access:** Authenticating and securely interacting between applications.
- **Database Access:** Managing secure connections to databases.
- **Server and Infrastructure Automation:** Performing tasks like backups, deployments, and system maintenance.
- **CI/CD Pipelines:** Supporting build, test, and deployment workflows.
- **Cloud Environments:** Managing resources across cloud or hybrid platforms.
- **Secrets Management:** Retrieving sensitive credentials or configurations securely.

These scenarios highlight the critical role of service accounts in enabling secure, automated, and efficient operations.

3. Background

NIST SP 800-207 defines Zero Trust Architecture (ZTA) as a security model where no entity, whether inside or outside the network perimeter, is inherently trusted. This principle extends to service accounts—non-human accounts used by applications, services, or automated processes—which, if improperly managed, can expose the organization to risks such as unauthorized access or privilege escalation.

4. Guidelines

Service accounts are allowed in a Zero Trust environment. The overall requirement is to use only approved certificate-based authentication and require the service account to be individually identifiable to the application calling the service for information. The guidelines for service accounts based on NIST SP 800-27 are as follows:

1. Apply the Principle of Least Privilege (PoLP)

- Align with NIST SP 800-207's recommendation to minimize access by assigning service accounts only the permissions required to fulfill specific functions.
- Periodically review and adjust permissions to prevent privilege creep.

2. Centralized Identity and Access Management (IAM)

- Use only VA approved IAM solutions in accordance with SP 800-207 to manage service account identities.
- Ensure each service account has a uniquel identifier.

3. Strong Authentication Mechanisms

- Replace static passwords with secure methods such as public key infrastructure (PKI) or certificate-based authentication as outlined in NIST SP 800-207.
- Enforce multifactor authentication (MFA) for all privileged service accounts.

4. Micro-Segmentation and Resource Isolation

- Leverage network segmentation to isolate service accounts, ensuring compliance with the resource-centric access controls described in SP 800-207.
- Define granular access policies to restrict interactions between service accounts and sensitive resources.

5. Dynamic Access Control and Policy Enforcement

- Implement dynamic access controls to continuously evaluate the trustworthiness of service accounts, as recommended in SP 800-207.
- Use contextual information, such as location and behavior, to enforce conditional access policies.

6. Lifecycle Management

- Automate the lifecycle of service accounts -- creation, renewal, termination, and periodic access review -- in line with NIST's emphasis on minimizing attack surfaces.
- Conduct regular reviews to identify and remove stale or unused service accounts.

7. Monitoring and Real-Time Visibility

- Continuously monitor service account activities for anomalies, as recommended in NIST SP 800-207, to enhance proactive threat detection.

- Use robust logging and Security Information and Event Management (SIEM) systems to track and analyze service account behavior.

8. Credential Management

- Rotate service account credentials regularly and enforce expiration dates, as recommended in SP 800-207.
- Avoid storing credentials in code repositories; instead, use secure secrets management solutions, such as the VA Privileged Access Solution (PAS).
- Use an approved VA Software Factory Utility for secrets management, which includes the VA PAS, to manage elevated access for service accounts, in alignment with NIST's focus on preventing privilege misuse: Utilities Starter Guide | CODE VA.

5. Responsibilities

- **System Administrators:** Enforce policies for service account lifecycle management and secure access.
- **IT Security Team:** Monitor compliance with ZTA principles, conduct regular audits, and respond to detected anomalies.
- **Application Developers:** Integrate service account authentication securely by using secrets management tools and adhering to SP 800-207 guidance.

6. References

- Service Account Password Rotation Policy Change announcement (Internal)
- Access Control Policy (Internal)
- VA Identification and Authentication (IA) Policy (Internal)
- Enterprise Active Directory User Account Management SOP (Internal)
- VA Privileged Access Management (SOPs) (Internal)

Document Version Control

Date	Version	Change Details	By
2/28/2025	1.0	Initial release for FY25	OCTO/TAS
3/16/2026	2.0	Update containing links to PAS and FY26 changes	OCTO/TAS