ARCHITECTURE

Identity & Access Management

IAM Architecture, Privileged Access & Identity Governance

Comprehensive IAM guide covering identity architecture, authentication protocols, privileged access management, identity governance and administration, federation, and implementing least privilege at scale.

HORIZONSHIELD

LEVEL
Intermediate

READ TIME
40 min

SERIES
Book 17 of 22

Contents

CHAPTER 01

IAM Architecture Fundamentals

Identity is the new perimeter. As networks dissolve into cloud, remote work, and SaaS, the question "who is accessing what" has become more important than "where is the request coming from." Effective IAM architecture answers that question with precision and speed, at every access decision.

IAM Component	Function	Example Technologies
Identity Provider (IdP)	Authoritative source of user identities	Microsoft Entra ID, Okta, Ping Identity
Directory Service	Store and manage user and group objects	Active Directory, LDAP, Azure AD DS
Authentication Service	Verify identity claims	ADFS, Okta, Auth0, Keycloak
Authorisation Service	Determine access rights for authenticated identity	OPA, Casbin, Azure RBAC, AWS IAM
PAM Solution	Control and monitor privileged access	CyberArk, BeyondTrust, HashiCorp Vault
IGA Platform	Govern identity lifecycle and access rights	SailPoint, Saviynt, One Identity
MFA Provider	Add second factor to authentication	Duo, Microsoft Authenticator, YubiKey

! Service accounts are the most dangerous and most neglected identity type in most organisations. They accumulate excessive permissions over time, share credentials across teams, rarely have MFA, and are never offboarded. Audit every service account in your environment — you will find accounts running critical workloads with domain admin privileges assigned years ago by someone who no longer works there.

The principle of least privilege — granting only the permissions required to perform a specific task, for only the time required — is simple to state and difficult to implement at scale. Role explosion (too many fine-grained roles), access creep (permissions accumulating over a career), and emergency access (break-glass accounts) all erode least privilege over time. Identity Governance and Administration (IGA) tools automate the ongoing work of access certification and lifecycle management that least privilege requires.

CHAPTER 02

Authentication Protocols

This chapter covers authentication protocols — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

SAML 2.0, OAuth 2.0, OpenID Connect, and FIDO2 deep dives. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 03

Privileged Access Management

This chapter covers privileged access management — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

PAM architecture, just-in-time access, session recording, and vault design. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 04

Identity Governance & Administration

This chapter covers identity governance & administration — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

Role engineering, access certifications, and Joiner-Mover-Leaver process. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 05

Multi-Factor Authentication at Scale

This chapter covers multi-factor authentication at scale — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

MFA deployment strategy, phishing-resistant options, and exception handling. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 06

Federation & Single Sign-On

This chapter covers federation & single sign-on — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

SAML federation, OIDC, cross-tenant trust, and SSO architecture. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 07

Non-Human Identity Management

This chapter covers non-human identity management — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

Service accounts, API keys, secrets, and workload identity federation. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

HS

HORIZONSHIELD ORIGINALS

Complete Security Library

Practitioner-written guides for real-world security implementation.

AVAILABLE IN THIS SERIES

01	SMB Cybersecurity Guide	02	Penetration Testing Checklist
03	Incident Response Playbook	04	DORA Compliance Guide
05	Cloud Security Hardening	06	Zero Trust Architecture
07	Threat Hunting & SOC Operations	08	DevSecOps Implementation
09	Web Application Security	10	Network Security Fundamentals
11	Linux & Systems Security	12	Social Engineering & Human Hacking
13	Malware Analysis & Reverse Engineer…	14	Digital Forensics & Incident Respon…
15	Applied Cryptography	16	Compliance Audit & Risk Management
17	**Identity & Access Management**	18	Threat Intelligence Operations
19	Red Team Operations	20	OT & ICS Security
21	Privacy Engineering & Data Protecti…	22	AI Security & LLM Threats

horizonshield.net/library

Download all 22 books · Access hands-on labs · Track your progress

Published Q1 2026 · Updated annually