Zero Trust (ZT) Overview

David L. Voelker

DON CISO Team

DON CIO Zero Trust Lead

Champions: CTO/CISO

HQCA-2023-A-113// Distribution A: For Public Release; Unlimited Distribution

What is zero trust?

Definition (from EO 14028):

Sec. 10 Definitions for the purpose of the order: (k) the term “Zero Trust Architecture” means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources

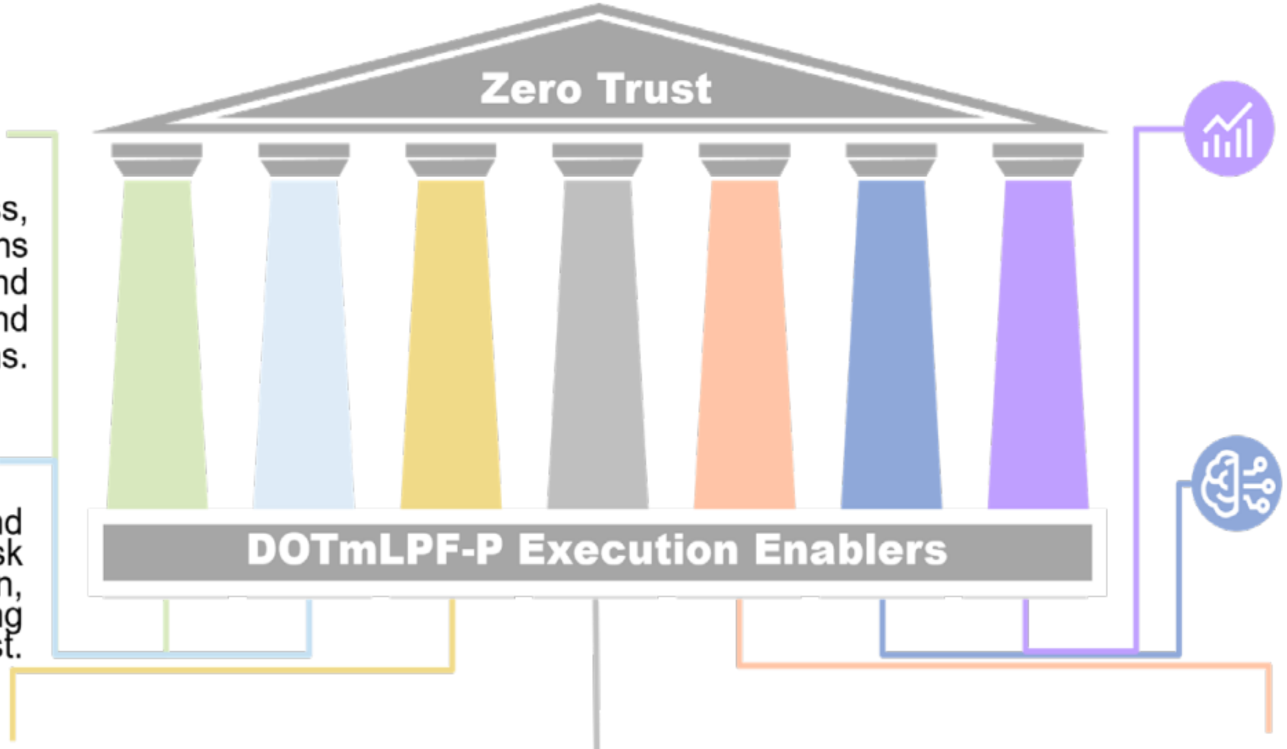
Key concepts:

- Threats exist both **inside and outside traditional network boundaries**
- The Zero Trust Architecture security model **assumes that a breach is inevitable** or has **likely already occurred**
  - Constantly limits access to only what is needed
  - Looks for anomalous or malicious activity
- Focus on **protecting data in real-time** within a dynamic threat environment
- **Data-centric security model**
  - **Least privileged access** applied for every access decision
  - **Who, what, when, where, and how** are critical for appropriately allowing or denying access

DoD ZT Courses of Action (COAs)

- COA #1: Brownfield legacy transformation is the most complex and resource intensive to implement ZT; 3-5 year plan
  - **DoD ZT PfMO recommends targeting funding here as of 13 JUN 2022**
- COA #2: Commercial cloud options AWS, Azure, Goggle, Oracle, IBM, etc.
  - DON CTO Leadership planning to demonstrate Flank Speed's ZT capabilities in partnership with the ZT PfMO's review of Microsoft Azure
- COA #3: On-Premises Private Cloud Implementation
  - Government designed Native Zero Trust Cloud (NZTC)
    - Realistic approach to implementing ZT

DoD Zero Trust Capability Pillars



User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Devices

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.

Applications & Workloads

Secure everything from Applications to hypervisors, to include the protection of containers and virtual machines.

Data

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Network & Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.

Visibility & Analytics

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Automation & Orchestration

Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Naval View: Implement Zero Trust

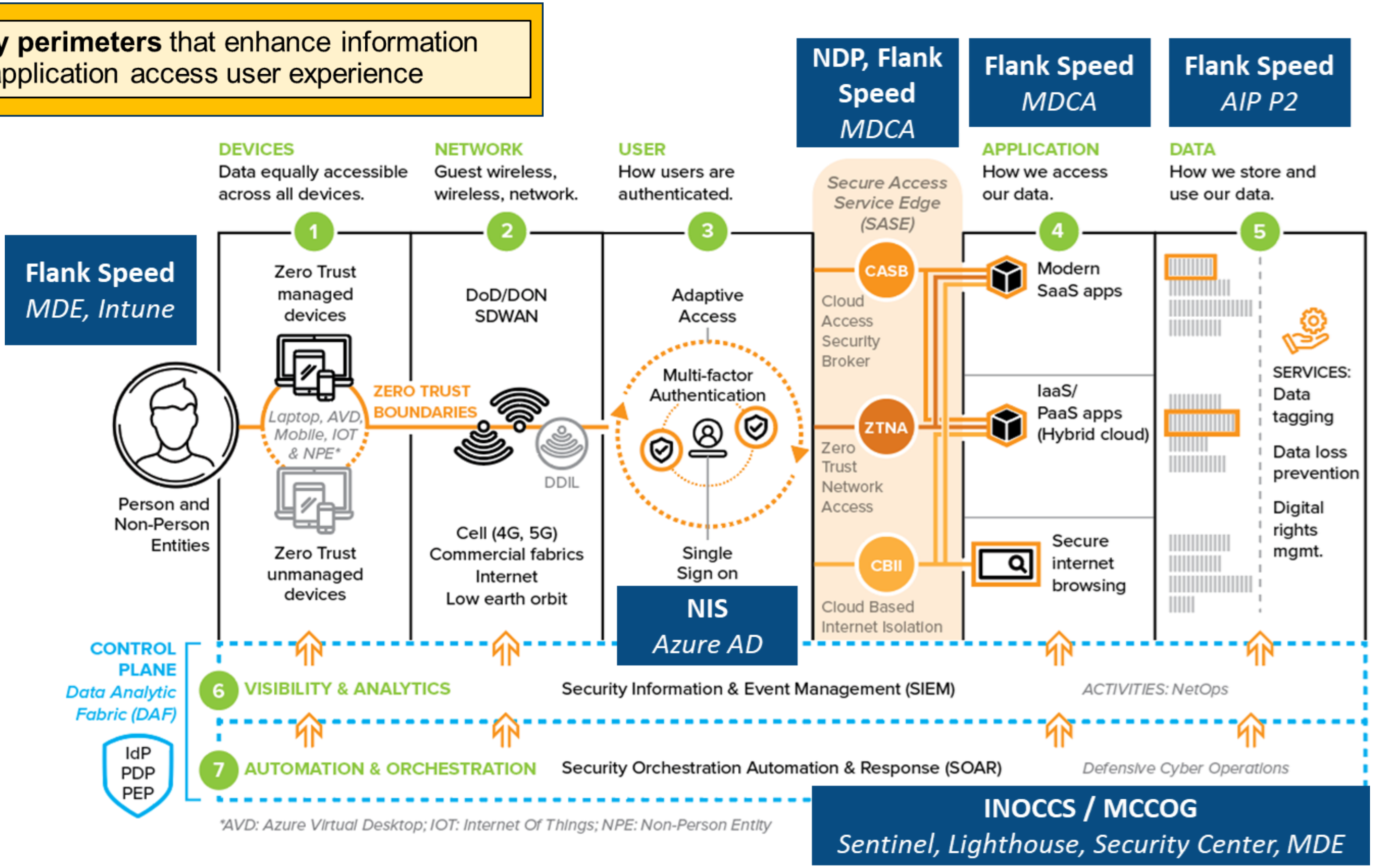
Strategic Objective

Establish **dynamic identity perimeters** that enhance information security and the data/application access user experience

Subordinate objectives

- Enable dynamic user access and resource visibility
- Provide secure and broad access across networks and devices
- Conditionally authorize access to multiple categories of information
- Unify and automate cyber defense and network operations

Not hypothetical… Operating *today*, improving *now*



Flank Speed *MDE, Intune*

NDP, Flank Speed *MDCA*

Flank Speed *MDCA*

Flank Speed *AIP P2*

DEVICES Data equally accessible across all devices.

NETWORK Guest wireless, wireless, network.

USER How users are authenticated.

Secure Access Service Edge (SASE)

APPLICATION How we access our data.

DATA How we store and use our data.

1 Zero Trust managed devices

Laptop, AVD, Mobile, IOT & NPE*

Zero Trust unmanaged devices

Person and Non-Person Entities

ZERO TRUST BOUNDARIES

2 DoD/DON SDWAN

DDIL

Cell (4G, 5G) Commercial fabrics Internet Low earth orbit

3 Adaptive Access

Multi-factor Authentication

Single Sign on

NIS *Azure AD*

CASB Cloud Access Security Broker

ZTNA Zero Trust Network Access

CBII Cloud Based Internet Isolation

4 Modern SaaS apps

IaaS/ PaaS apps (Hybrid cloud)

Secure internet browsing

5 SERVICES: Data tagging

Data loss prevention

Digital rights mgmt.

CONTROL PLANE *Data Analytic Fabric (DAF)*

IdP PDP PEP

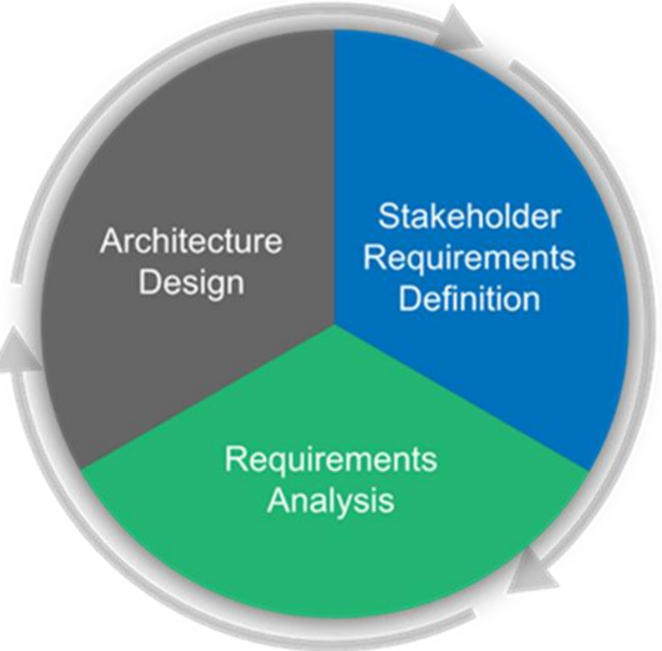
6 VISIBILITY & ANALYTICS Security Information & Event Management (SIEM) *ACTIVITIES: NetOps*

7 AUTOMATION & ORCHESTRATION Security Orchestration Automation & Response (SOAR) *Defensive Cyber Operations*

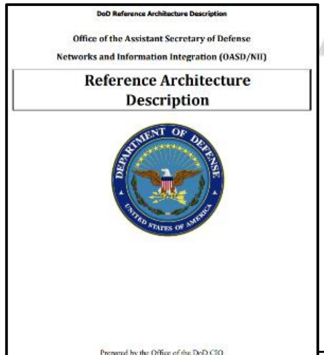
AVD: Azure Virtual Desktop; IOT: Internet Of Things; NPE: Non-Person Entity

INOCCS / MCCOG *Sentinel, Lighthouse, Security Center, MDE*

Initial Systems Engineering Technical Processes



- **Stakeholder Requirements Definition**
  - The Stakeholder Requirements Definition process translates stakeholder capability needs into a set of technical requirements.
  - Source Requirements:
    - DoD Zero Trust Reference Architecture v2.0
    - DoD Zero Trust Strategy
    - Zero Trust Capability Execution Roadmap
    - NIST 800-53, Security and Privacy Controls
    - NIST 800-162, ABAC
    - NIST 800-207, ZTA
    - Many more



DoD Reference Architecture Description

Office of the Assistant Secretary of Defense

Networks and Information Integration (OASD/NII)

Reference Architecture Description

Prepared by the Office of the DoD CIO

JUNE 2010

- **Requirements Analysis**
  - Requirements Analysis activities support allocation and derivation of requirements down to the system elements representing the lowest level of the design. The allocated requirements form the basis of contracting language and the system performance specification.
- **Architecture Design**
  - The Architecture Design process is iterative and strives to seek a balance among cost, schedule, performance, and risk that still meets stakeholder needs. Supports analysis of design considerations and enables reasoning about key system aspects and attributes such as reliability, maintainability, survivability, sustainability, performance, and total ownership cost.

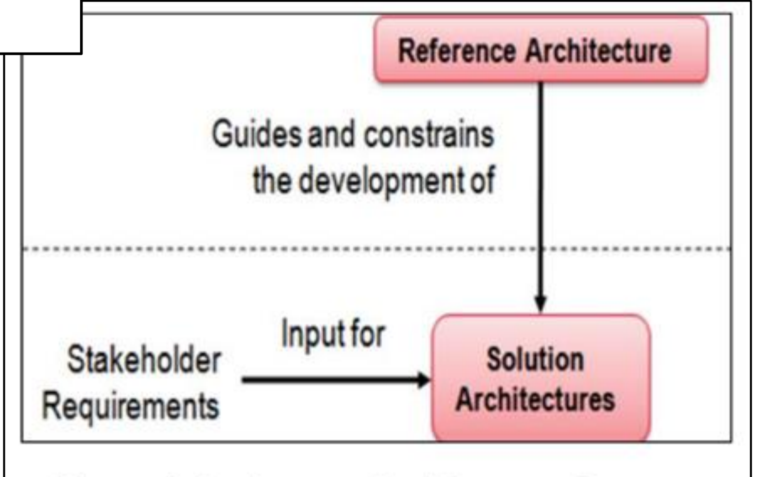
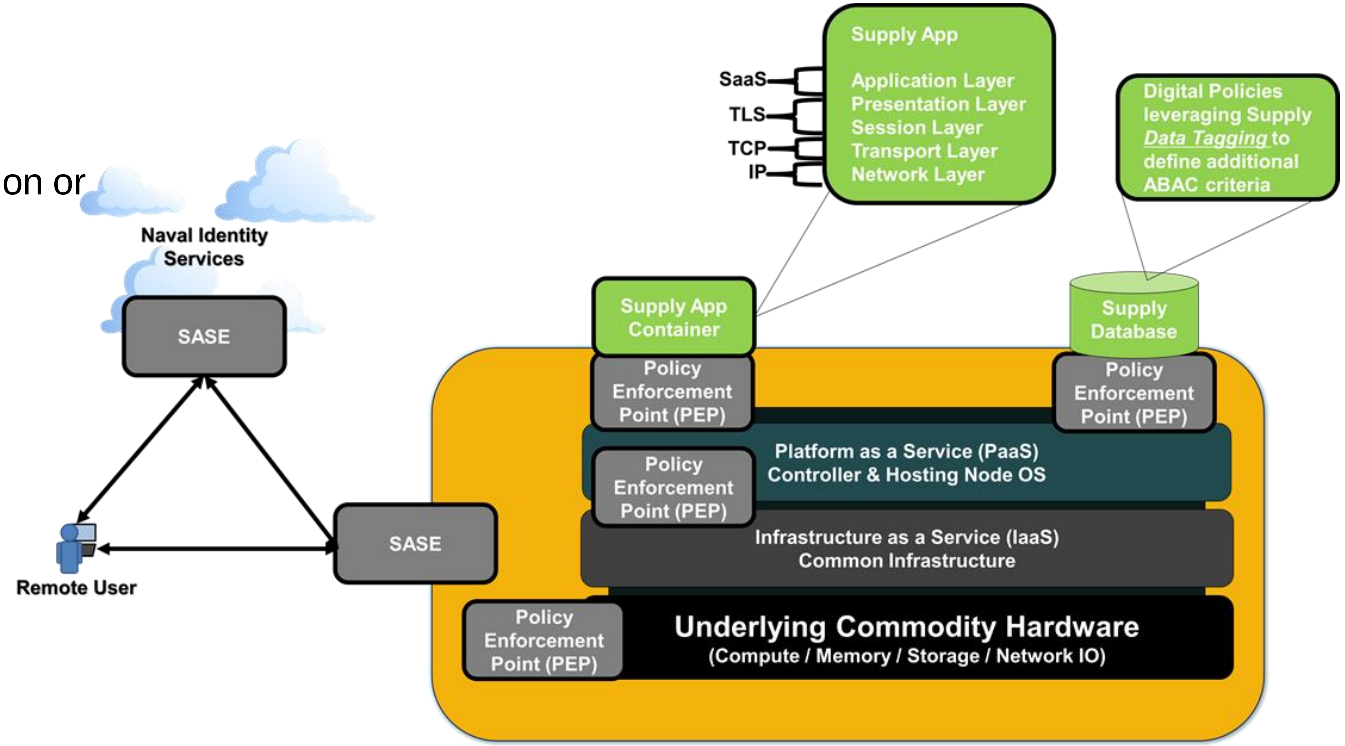


Figure 1 - Reference Architecture Purpose

Designing for Zero Trust

Repeatable process with reusable tools for any system in any environment

- Identify what you want to protect
- Define Mission Outcomes under the assumption of a hostile environment and presumption of breach
- Map transaction flows
  - Determine means of User, Device and Network access
- Design Architecture
  - Architect from the inside out
  - Develop Access Policies
  - Audit the technical baseline, identify HW/SW reconfiguration or replacement options and requirements
- Design Thinking Activities
  - Event Storming (Domain Driven Design)
  - Tabletop Mission Cyber Risk Assessments (TMCRAs)
- Prototype and Test
  - Validate Meta Polices prioritize access policies correctly
  - Always Verify Policy Permits
  - Automation & Orchestration
  - Unified analytics
    - User and Entity Behavioral Analytics (UEBA)
- Simplify the design as much as possible
- Monitor and Maintain
- Look for opportunities to improve the design


Naval Identity Services
SASE
SASE
Remote User
SaaS
TLS
TCP
IP
Supply App
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Digital Policies leveraging Supply *Data Tagging* to define additional ABAC criteria
Supply App Container
Supply Database
Policy Enforcement Point (PEP)
Policy Enforcement Point (PEP)
Platform as a Service (PaaS) Controller & Hosting Node OS
Policy Enforcement Point (PEP)
Infrastructure as a Service (IaaS) Common Infrastructure
Policy Enforcement Point (PEP)
Underlying Commodity Hardware
(Compute / Memory / Storage / Network IO)

Operational Concept

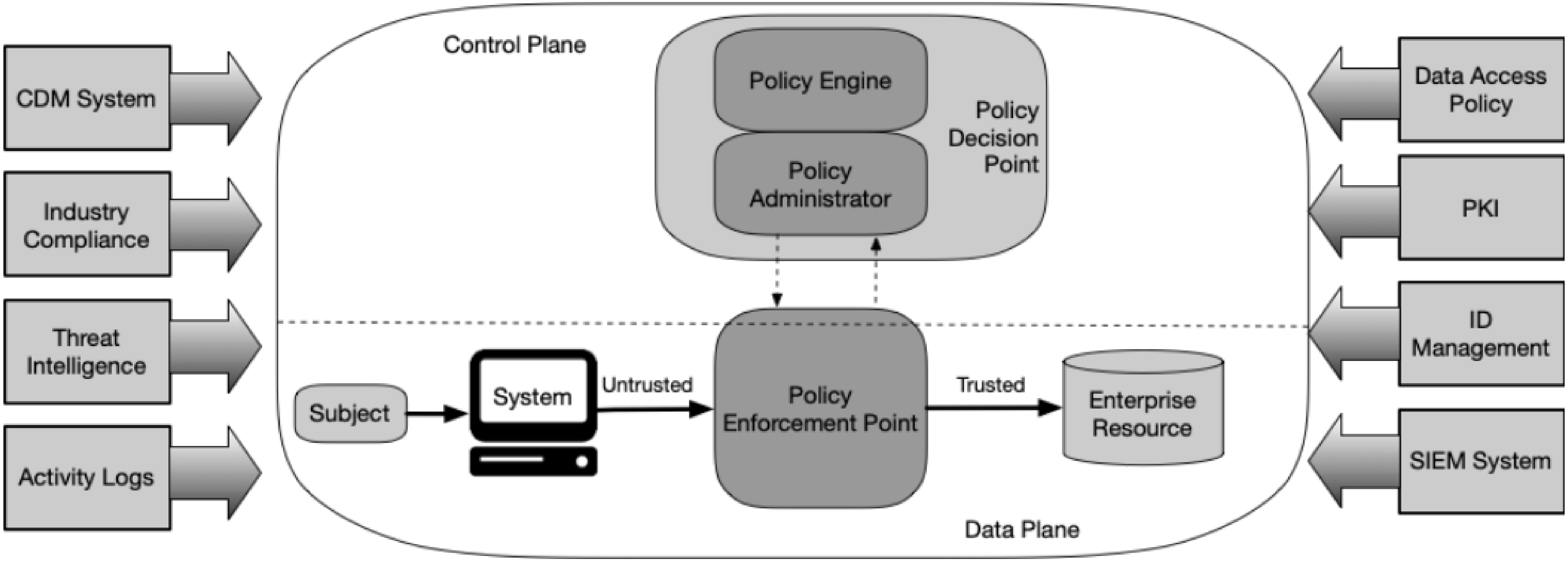
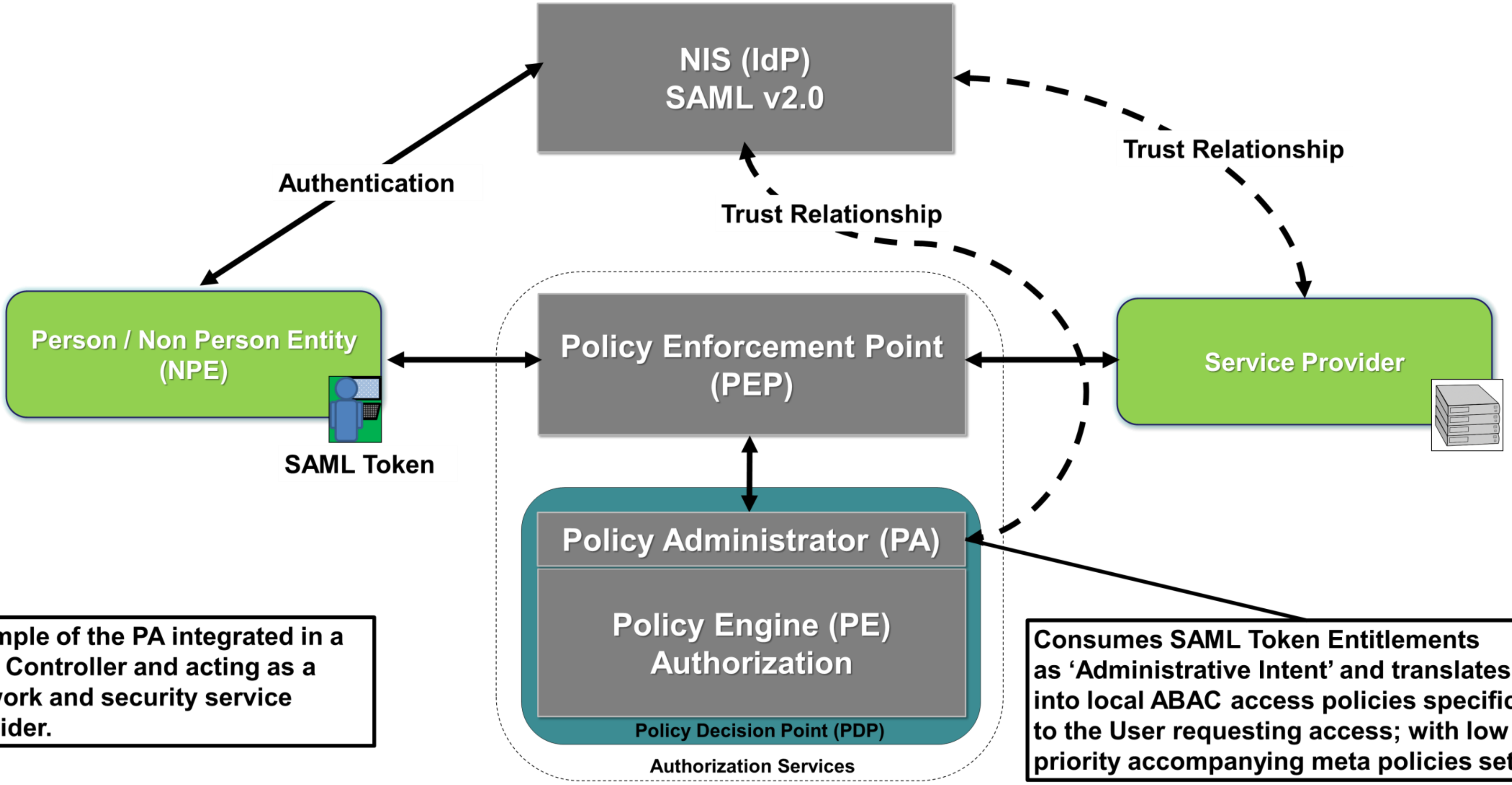


Figure 2: Core Zero Trust Logical Components

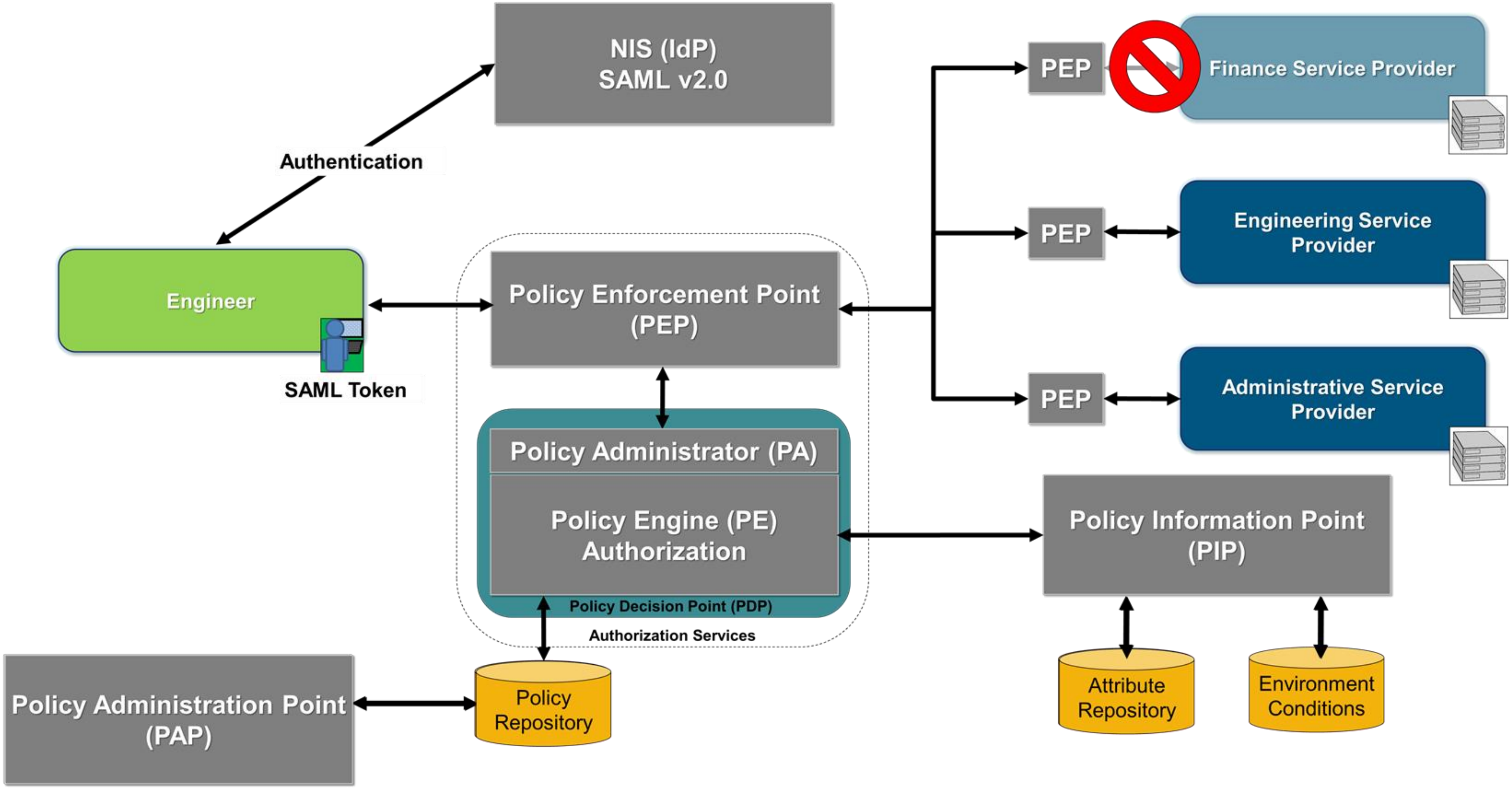
Naval Identity Services (NIS) ICAM Interoperability


NIS (IdP)
SAML v2.0
Authentication
Trust Relationship
Trust Relationship
Person / Non Person Entity (NPE)
SAML Token
Policy Enforcement Point (PEP)
Service Provider
Policy Administrator (PA)
Policy Engine (PE) Authorization
Policy Decision Point (PDP)
Authorization Services

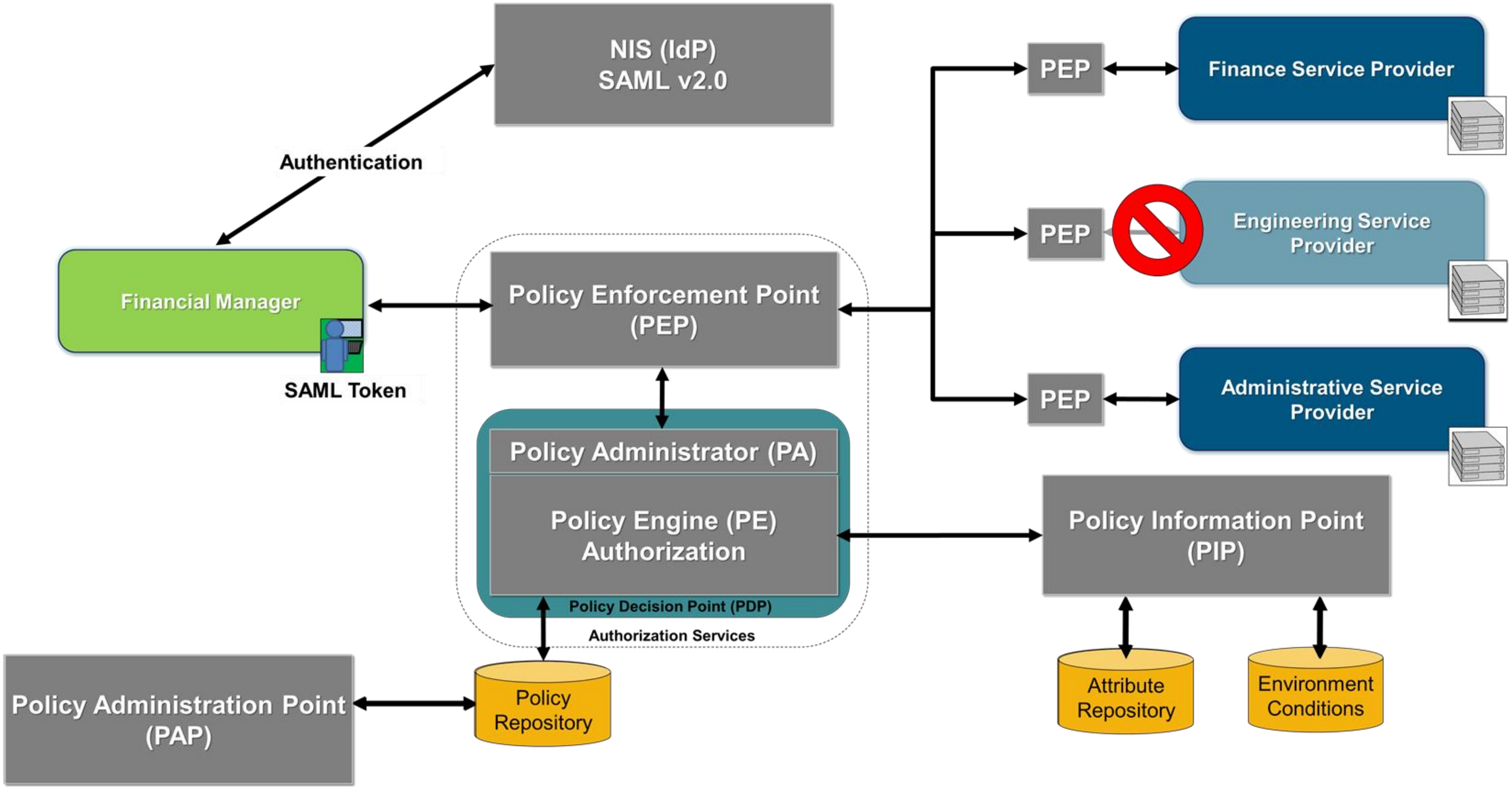
Example of the PA integrated in a SDN Controller and acting as a network and security service provider.

Consumes SAML Token Entitlements as ‘Administrative Intent’ and translates into local ABAC access policies specific to the User requesting access; with low priority accompanying meta policies settings

Zero Trust Access Management Outcome One


NIS (IdP)
SAML v2.0
Authentication
Engineer
SAML Token
Policy Enforcement Point (PEP)
Policy Administrator (PA)
Policy Engine (PE) Authorization
Policy Decision Point (PDP)
Authorization Services
PEP
Finance Service Provider
PEP
Engineering Service Provider
PEP
Administrative Service Provider
Policy Information Point (PIP)
Attribute Repository
Environment Conditions
Policy Administration Point (PAP)
Policy Repository

Zero Trust Access Management Outcome Two


NIS (IdP)
SAML v2.0
Authentication
Financial Manager
SAML Token
Policy Enforcement Point (PEP)
Policy Administrator (PA)
Policy Engine (PE) Authorization
Policy Decision Point (PDP)
Authorization Services
Policy Administration Point (PAP)
Policy Repository
PEP
Finance Service Provider
PEP
Engineering Service Provider
PEP
Administrative Service Provider
Policy Information Point (PIP)
Attribute Repository
Environment Conditions

Governance & Implementation Coordination

DON CIO ZT Actions

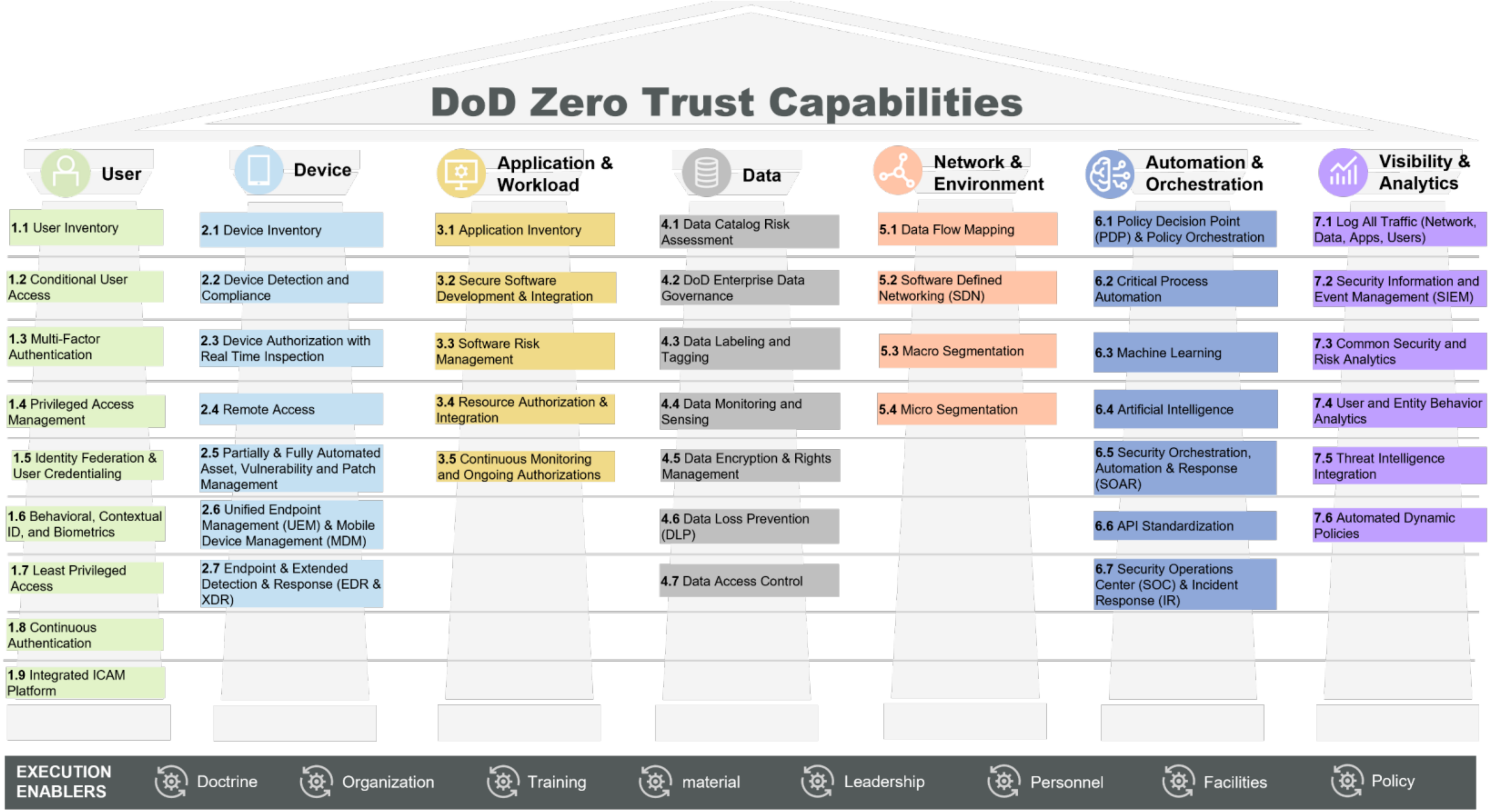
- Strategic Intent for Zero Trust Implementation
- DON CIO Zero Trust Major Design Concept
- DON Zero Trust Implementation Plan

▼ Coordination POCs

- DON Chief Information Security Officer, Mr. Alvin (Tony) Plater, at alvin.a.plater3.civ@us.navy.mil
- DON Chief Technology Officer, Mr. Justin M. Fanelli, at justin.m.fanelli.civ@us.navy.mil
- DON Chief Engineer, Mr. Carroll (Rick) Quade, at carroll.p.quade.civ@us.navy.mil

Questions

DoD Zero Trust Capabilities



DoD Zero Trust Capabilities

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

EXECUTION ENABLERS: Doctrine · Organization · Training · material · Leadership · Personnel · Facilities · Policy