Innovating at the Edge Meetup, Aug ‘22

Securing Infrastructure for Edge Native Applications and Services

Anurag Ranjan

Intel Smart Edge Cloud Software Architect and PdM

intel®

Notices and Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

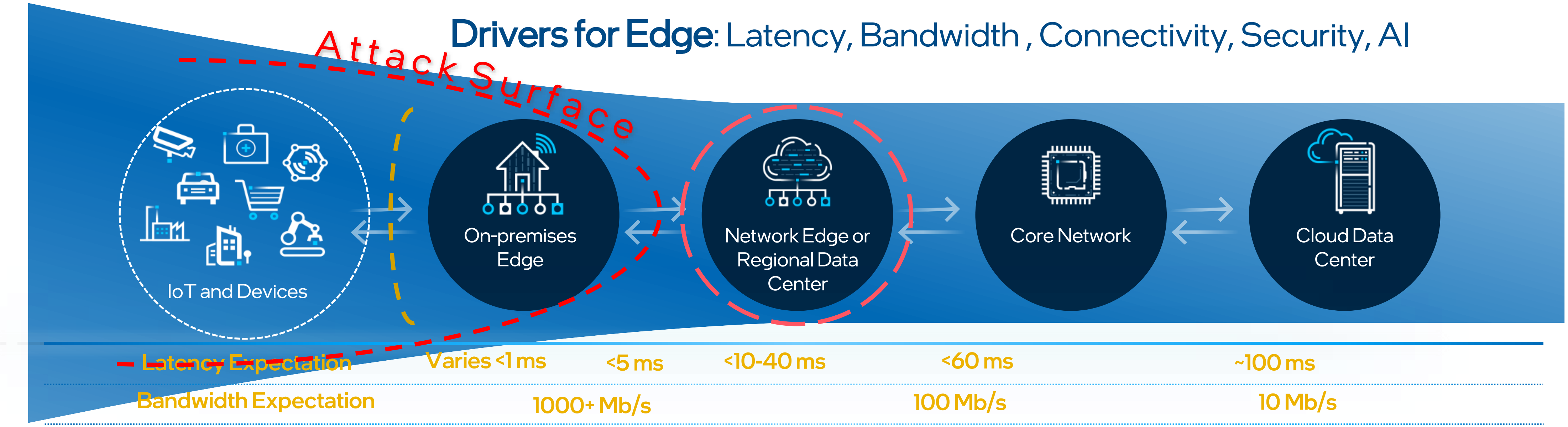
Overview

1. Motivation for Edge Computing : 5 mins
2. Security Threat Posture at the Edge : 10 mins
3. The approach to solving the challenges : 10 mins
4. Bundling into a package : 10 mins
5. References and Pointers : 5 mins

Edge Computing

intel®

Edge Native Platforms



Drivers for Edge: Latency, Bandwidth , Connectivity, Security, AI

Attack Surface

IoT and Devices

On-premises Edge

Network Edge or Regional Data Center

Core Network

Cloud Data Center

Latency Expectation	Varies <1 ms	<5 ms	<10-40 ms	<60 ms	~100 ms
Bandwidth Expectation		1000+ Mb/s		100 Mb/s	10 Mb/s

Opportunity @ the Edge by 2025

- Multi-access Edge and Private Wireless Hardware, Software, and Services - $29B [1]
- 75% of Data Created Outside Central Data Centers [2]

Key Technology Inflections

- Cloud Native Software
- Connectivity (5G, Multi-Access)
- Artificial Intelligence

Edge of the Future

- Real Time/Deterministic
- On-Demand/Dynamic
- Energy Efficient/Sustainable
- Massively Geo-Distributed at Scale
- Secure

Lower TCO with a consistent cloud native platform approach across edge locations

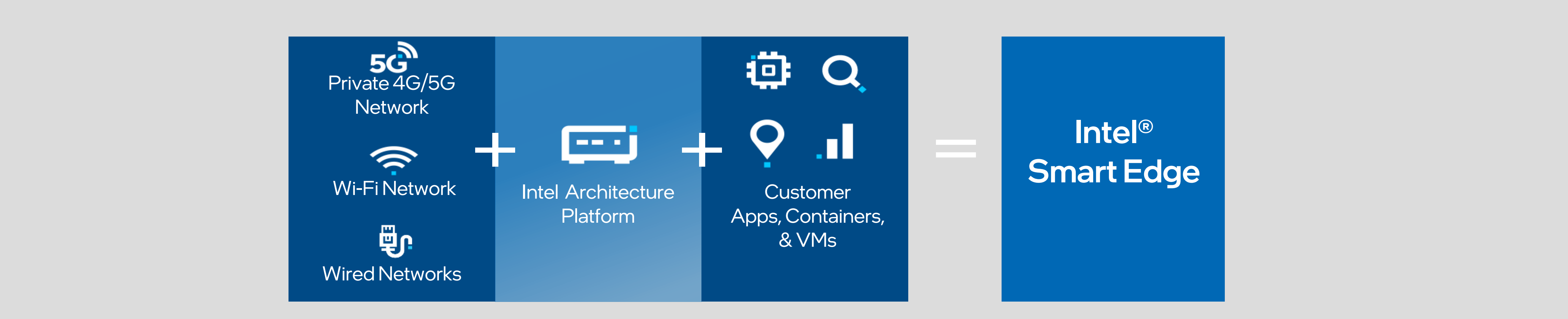
[1] MEC definition here refers to MEC2.0 hyperconverged edge. Source: IDC, Omdia, Intel Judgment.

[2] What Edge Computing Means for Infrastructure and Operations Leaders, Gartner, Oct 3, 2018.

Innovation at Edge using Intel® Smart Edge Platform

Build edge solutions faster and at lower cost

Simplify edge networking and application deployment with Intel® Smart Edge,
a software-defined platform that uses a certified Kubernetes engine to manage workloads, networking and abstract device complexities.



Private 4G/5G Network

Wi-Fi Network

Wired Networks

+ Intel Architecture Platform

+ Customer Apps, Containers, & VMs

= Intel® Smart Edge

Economics, Ease of Use, and Experience for Customers

Enable Critical Capabilities at the Edge

- Security
- 5G & Network Functions
- AI
- Media

Security Challenges

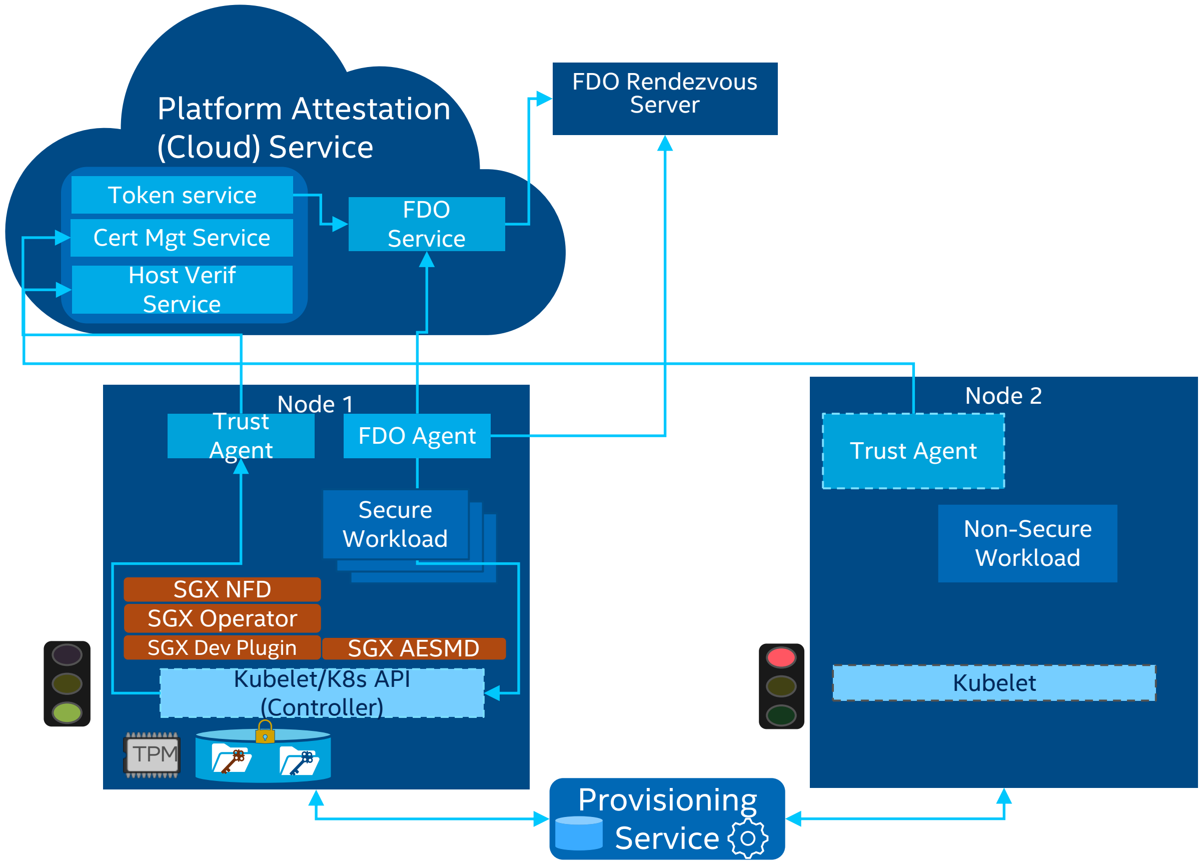
intel®

Security Posture for Edge Platform

1. Supply-chain vulnerability: Attacker adds malicious hardware/software components into a production system
2. Denial of Service Attack (DoS) and Distributed DoS (DDoS): Attacker overwhelms platform and network resources, denying access to genuine users
3. Tampering and Physical Attack: Attacker has physical access to the device and can tamper, steal vital cryptographic information, compromising service provider's infra
4. Snooping and Spoofing Attacks: Attacker gains unauthorized access to edge device/traffic and spoofs it to malicious content
5. Side Channel Attacks: Attacker uses advanced analysis of side channel information e.g. power, acoustic etc to compromise privacy
6. Unauthorized Control Access: Attacker compromises an unsecured device/host to get into a secure infrastructure accessible from it
7. Log Tampering: Attacker hampers observability by tampering unprotected log files
8. Privacy Leakage: Attacker gains access to personal information

Edge Compute Protection

Zero Trust Security Principles



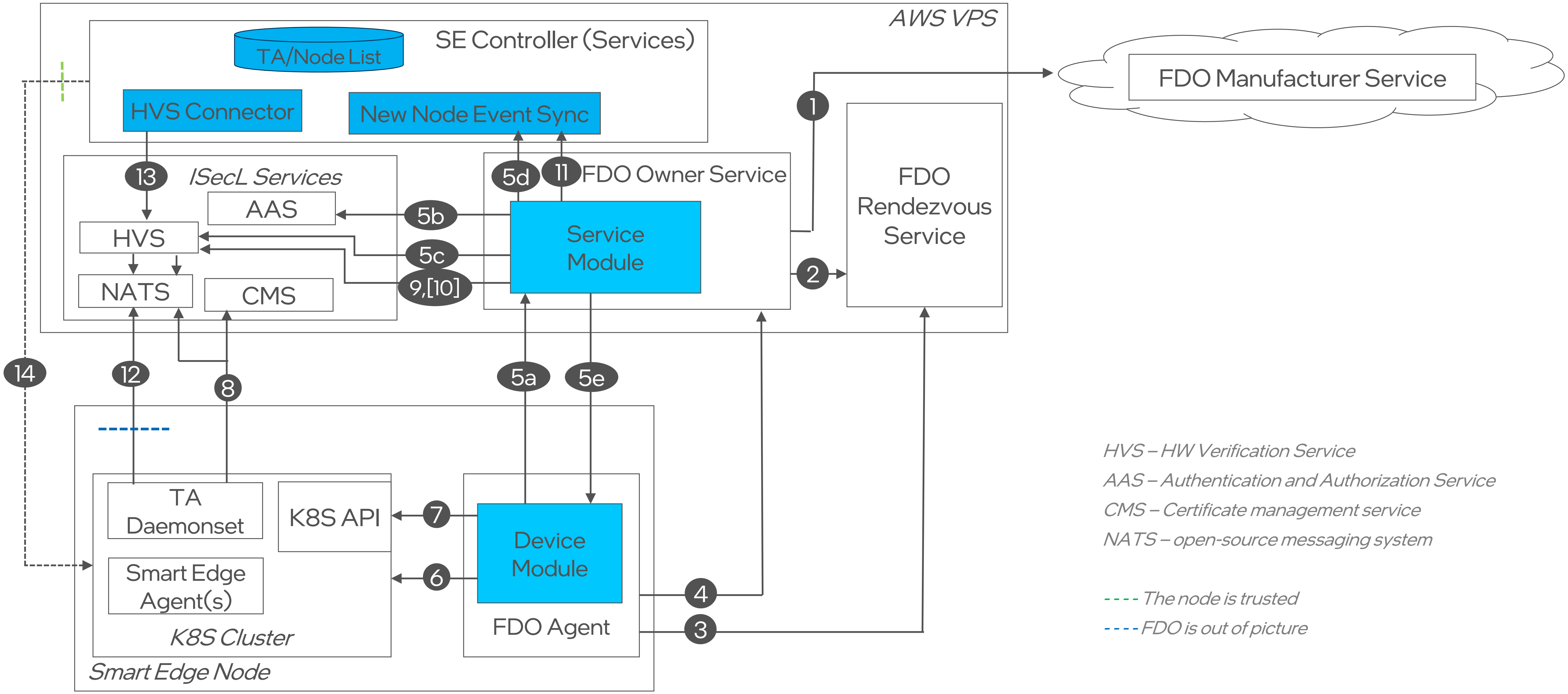
Key Features

- Secure On-Boarding and provisioning
- Platform integrity verification and attestation at boot time (using Intel® SecL - DC)
- Data at rest protection with LUKS full disk encryption (AES-NI accelerated)
- Secure Key Management and Caching
- SGX attestation framework and workload isolation

Usage

- Drop ship server to field for deployment, where it comes up, gets authenticated, provisioned and registered as a secure node.
- Tenant provisions transport keys for secure use in case of connecting traffic stream.
- Tenant provisions a secure workload to run on the same trusted node.

Secure Onboarding: Credentials Stored in TPM



HVS – HW Verification Service

AAS – Authentication and Authorization Service

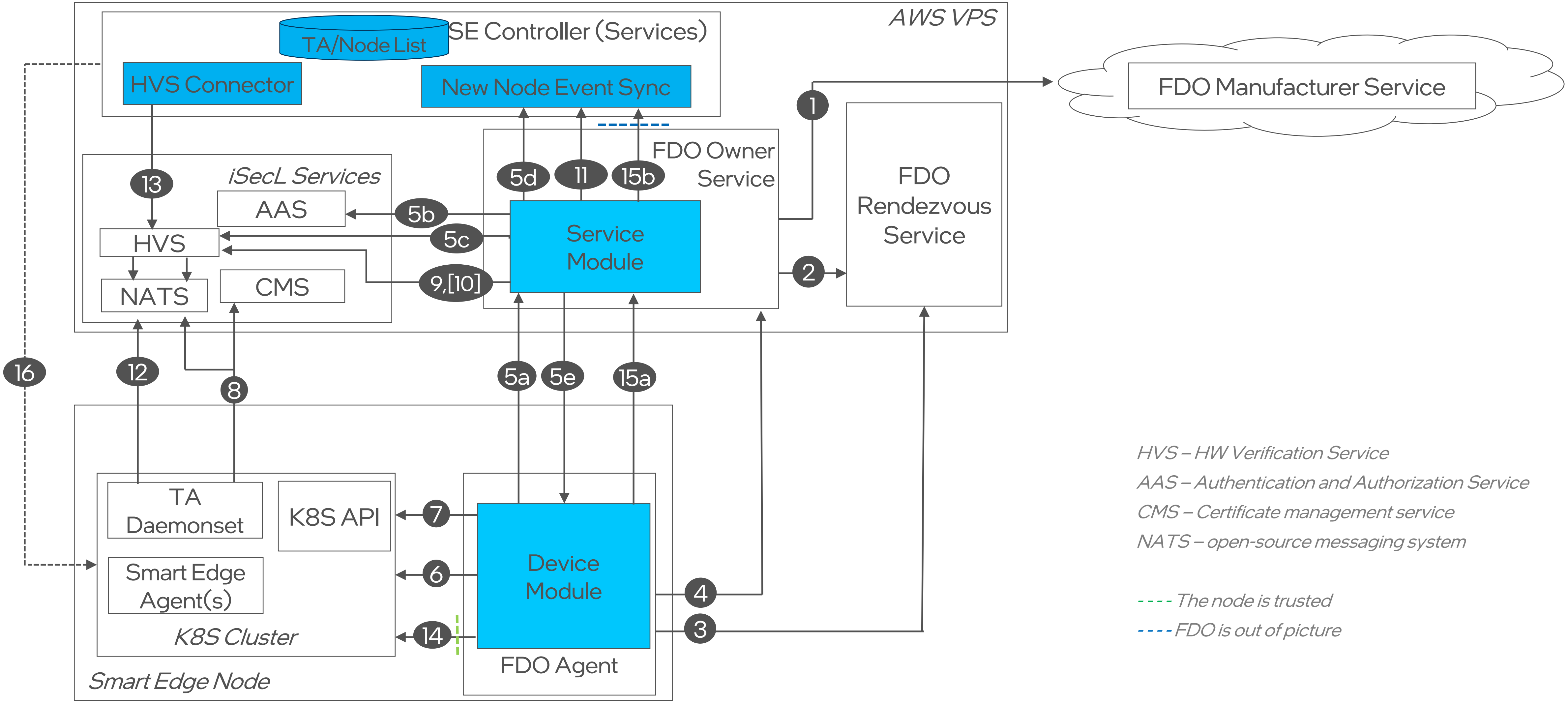
CMS – Certificate management service

NATS – open-source messaging system

- - - - *The node is trusted*

- - - - *FDO is out of picture*

Secure Onboarding: Node Credentials Generated



HVS – HW Verification Service

AAS – Authentication and Authorization Service

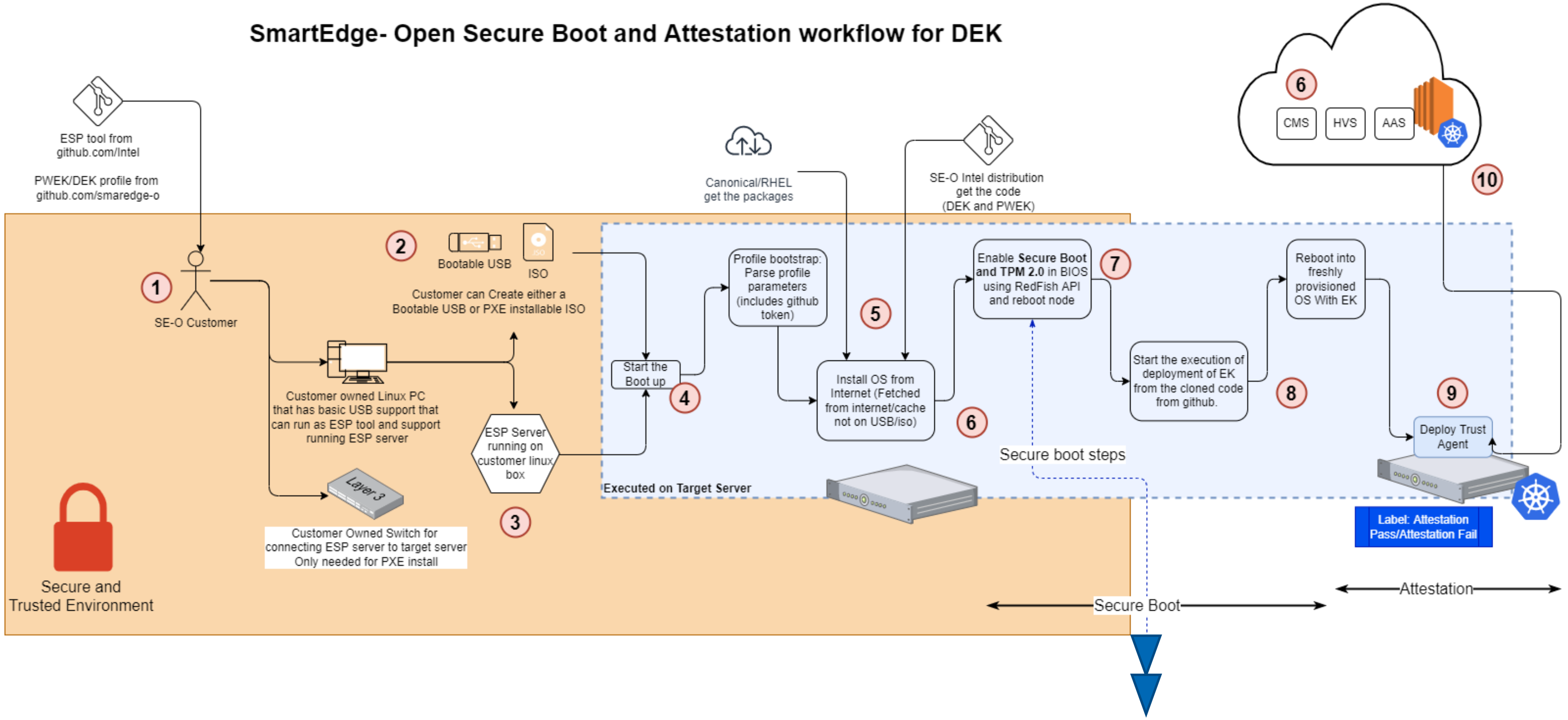
CMS – Certificate management service

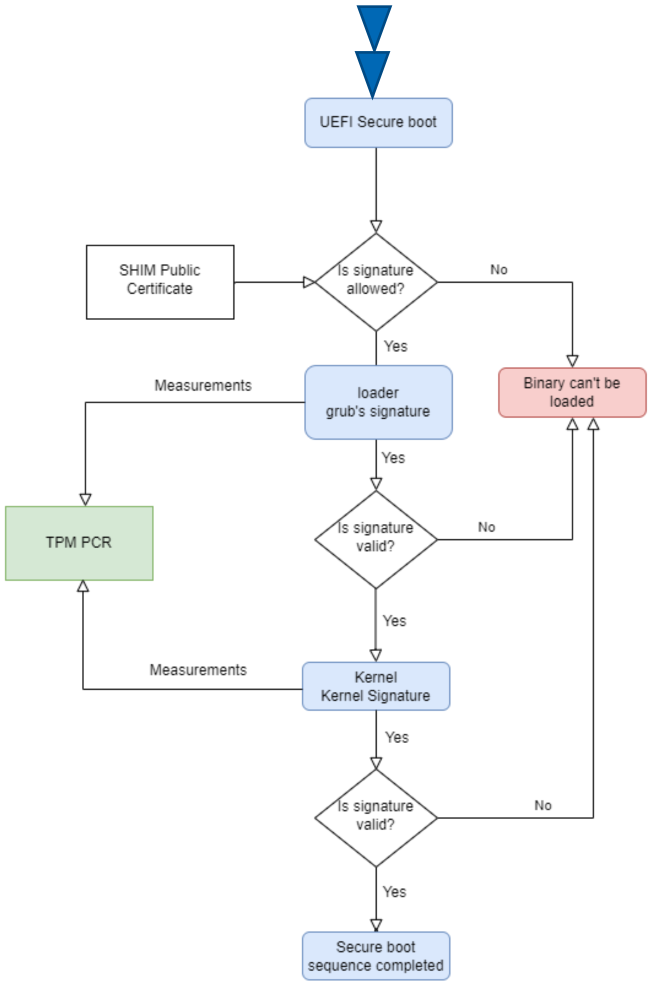
NATS – open-source messaging system

- - - - The node is trusted

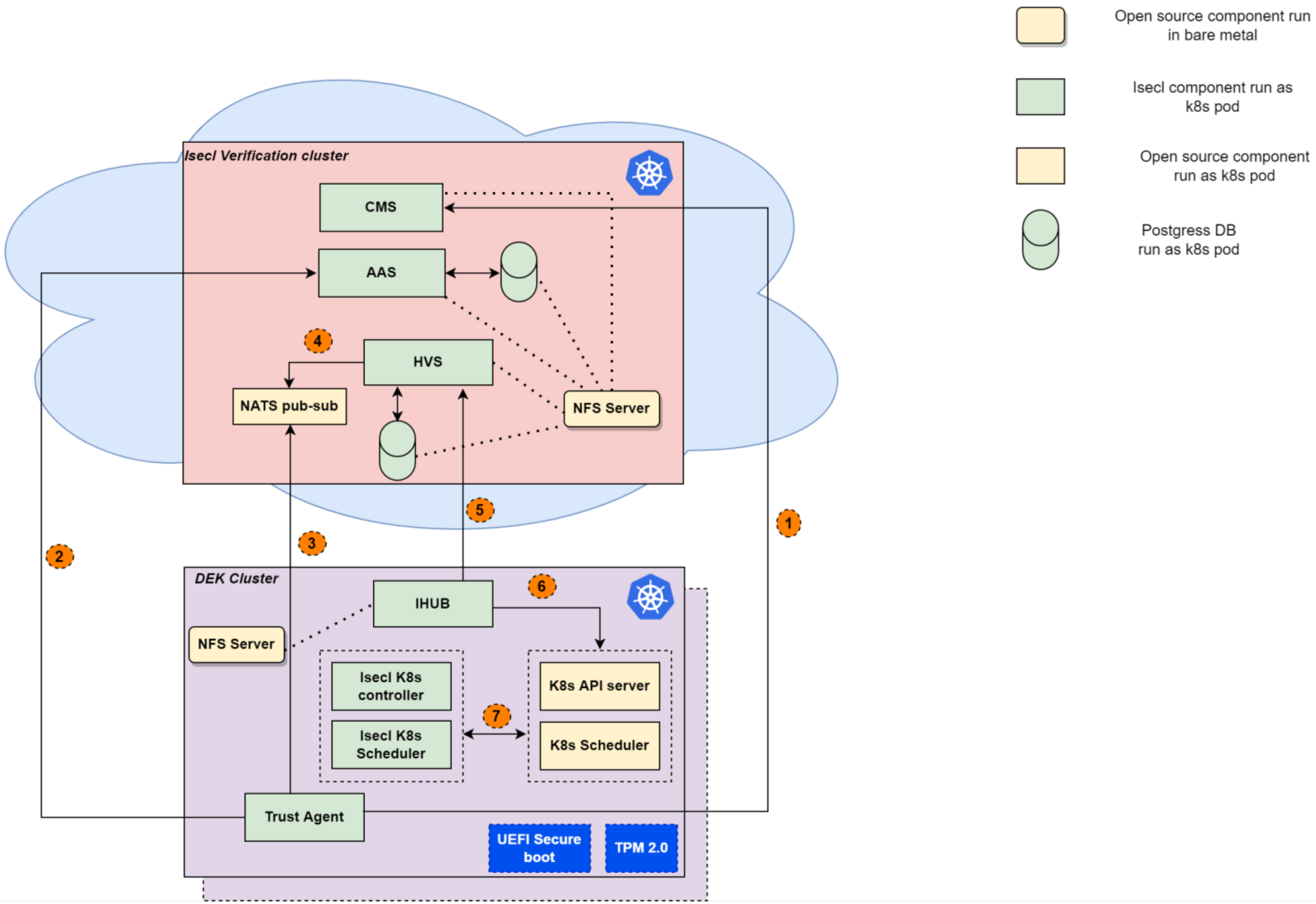
- - - - FDO is out of picture

Secure Boot and Attestation Workflow

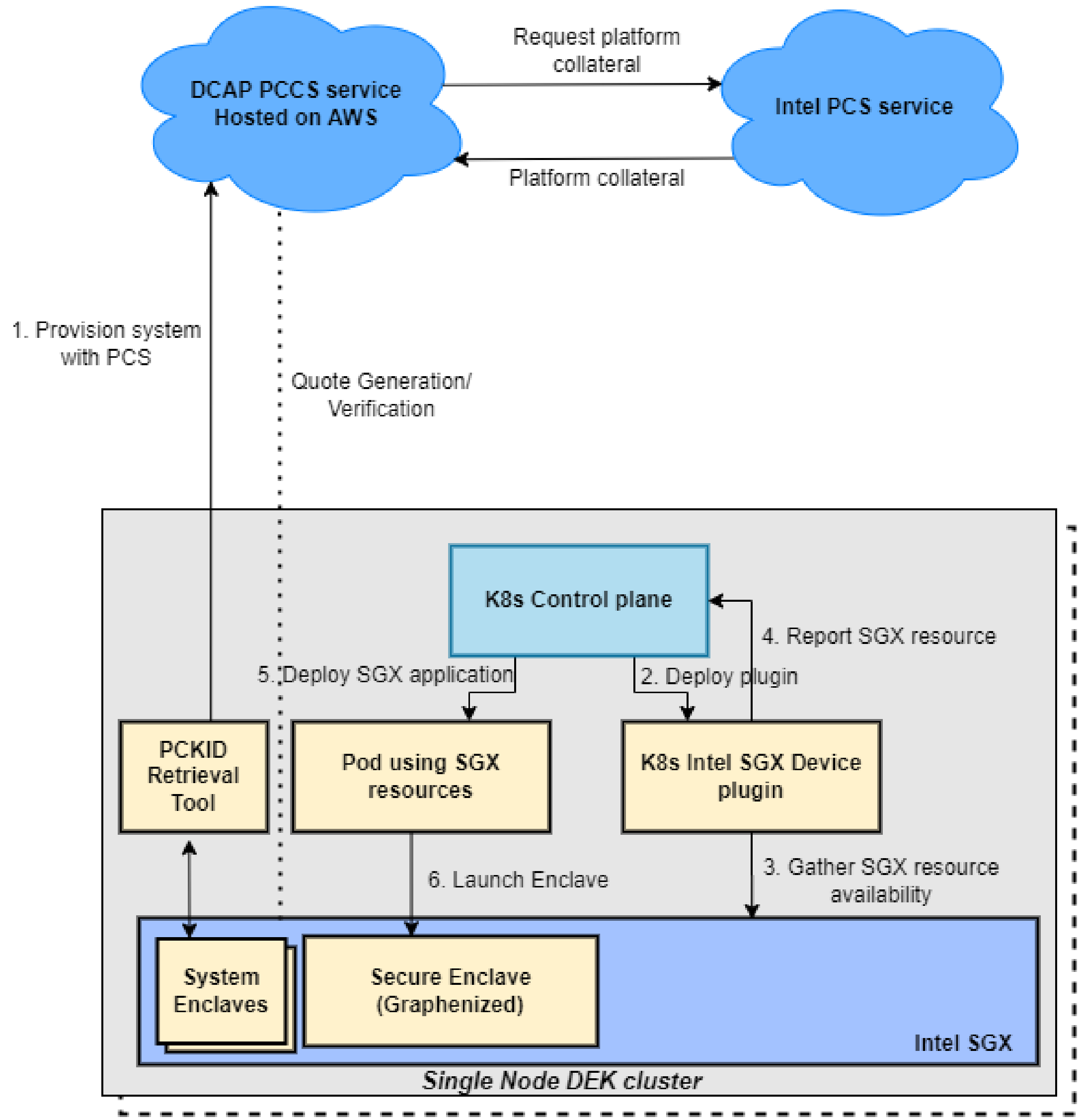

SmartEdge- Open Secure Boot and Attestation workflow for DEK
ESP tool from github.com/Intel
PWEK/DEK profile from github.com/smaredge-o
1
SE-O Customer
2
Bootable USB
ISO
Customer can Create either a Bootable USB or PXE installable ISO
Customer owned Linux PC that has basic USB support that can run as ESP tool and support running ESP server
ESP Server running on customer linux box
3
Layer 3
Customer Owned Switch for connecting ESP server to target server Only needed for PXE install
Secure and Trusted Environment
Canonical/RHEL get the packages
SE-O Intel distribution get the code (DEK and PWEK)
Start the Boot up
4
Profile bootstrap: Parse profile parameters (includes github token)
5
Install OS from Internet (Fetched from internet/cache not on USB/iso)
6
Enable Secure Boot and TPM 2.0 in BIOS using RedFish API and reboot node
7
Start the execution of deployment of EK from the cloned code from github.
8
Reboot into freshly provisioned OS With EK
9
Deploy Trust Agent
6
CMS
HVS
AAS
10
Secure boot steps
Executed on Target Server
Label: Attestation Pass/Attestation Fail
Secure Boot
Attestation

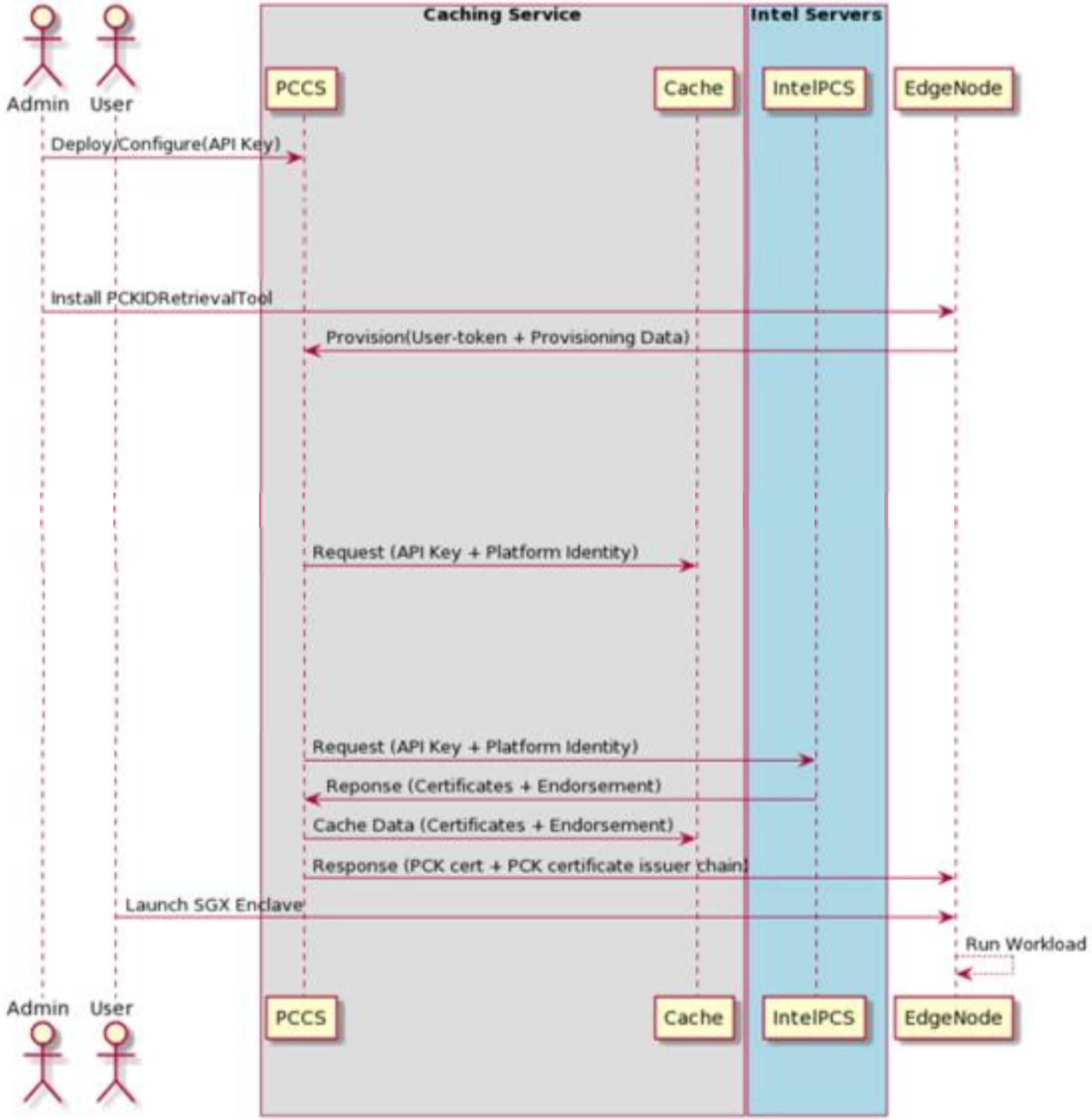


Platform Attestation using Intel® Security Libraries for Data Center (Intel® SecL- DC)



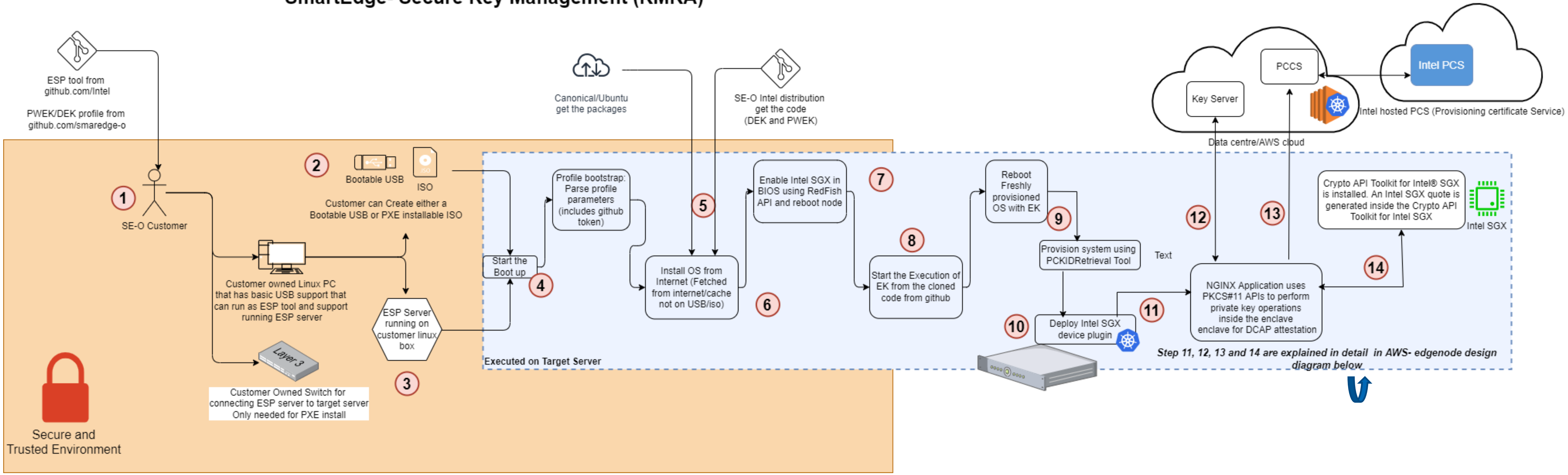
Creating Secure Enclave for Data in Use Protection




Caching Service
Intel Servers
Admin
User
PCCS
Cache
IntelPCS
EdgeNode
Deploy/Configure(API Key)
Install PCKIDRetrievalTool
Provision(User-token + Provisioning Data)
Request (API Key + Platform Identity)
Request (API Key + Platform Identity)
Reponse (Certificates + Endorsement)
Cache Data (Certificates + Endorsement)
Response (PCK cert + PCK certificate issuer chain)
Launch SGX Enclave
Run Workload
Admin
User
PCCS
Cache
IntelPCS
EdgeNode

Secure Key Management

SmartEdge- Secure Key Management (KMRA)



ESP tool from github.com/Intel

PWEK/DEK profile from github.com/smaredge-o

1 SE-O Customer

2 Bootable USB ISO

Customer can Create either a Bootable USB or PXE installable ISO

Customer owned Linux PC that has basic USB support that can run as ESP tool and support running ESP server

ESP Server running on customer linux box

3

Customer Owned Switch for connecting ESP server to target server Only needed for PXE install

Secure and Trusted Environment

Canonical/Ubuntu get the packages

SE-O Intel distribution get the code (DEK and PWEK)

Start the Boot up

4

Profile bootstrap: Parse profile parameters (includes github token)

5

Install OS from Internet (Fetched from internet/cache not on USB/iso)

6

Enable Intel SGX in BIOS using RedFish API and reboot node

7

8

Start the Execution of EK from the cloned code from github

Reboot Freshly provisioned OS with EK

9

Provision system using PCKIDRetrieval Tool

Text

10

Deploy Intel SGX device plugin

11

Executed on Target Server

Key Server

PCCS

Intel PCS

Intel hosted PCS (Provisioning certificate Service)

Data centre/AWS cloud

12

13

NGINX Application uses PKCS#11 APIs to perform private key operations inside the enclave enclave for DCAP attestation

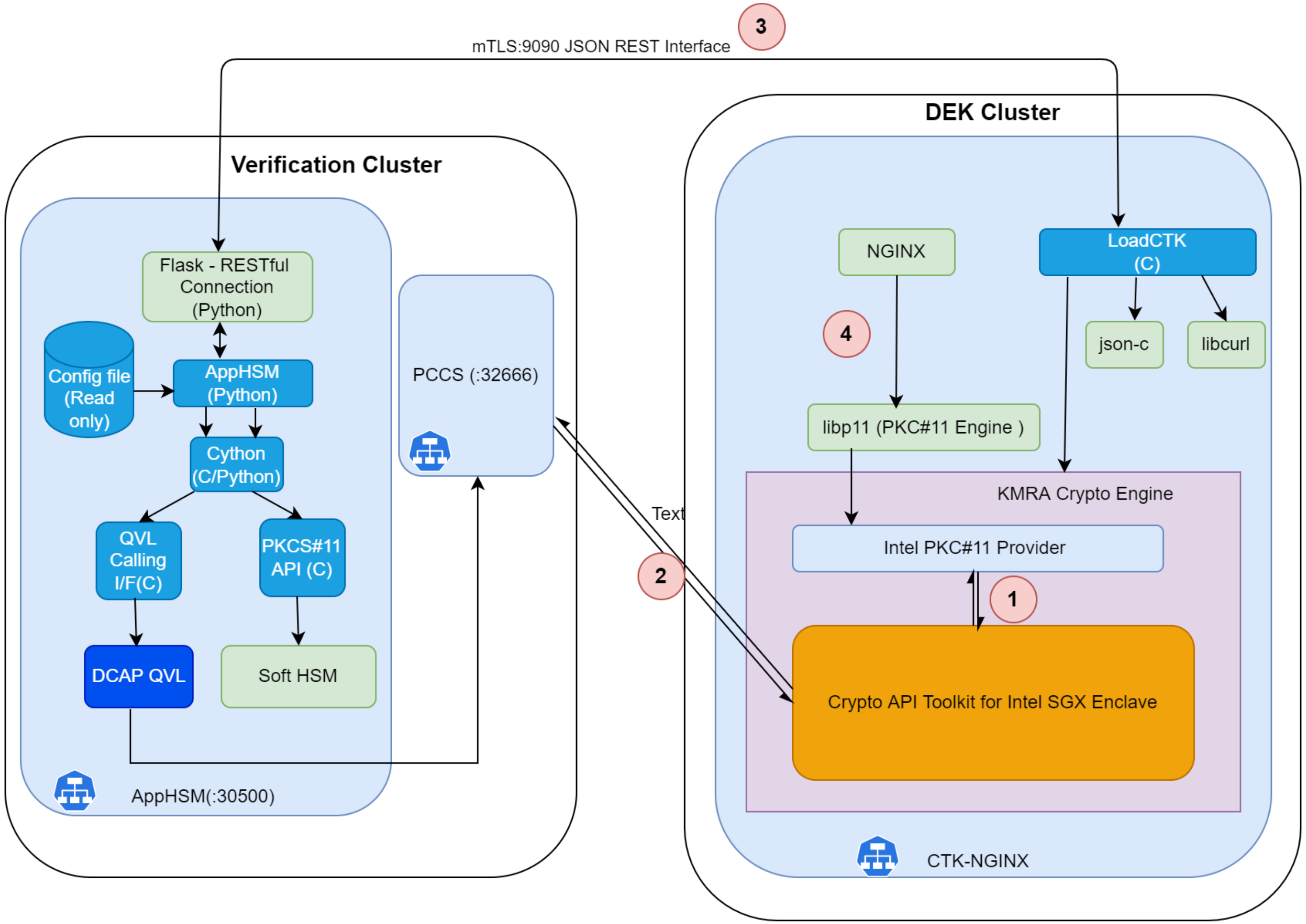
14

Crypto API Toolkit for Intel® SGX is installed. An Intel SGX quote is generated inside the Crypto API Toolkit for Intel SGX

Intel SGX

Step 11, 12, 13 and 14 are explained in detail in AWS- edgenode design diagram below

Secure Key Management



KMRA Reference Software

Open Source

Intel SGX Software

Secure Enclave

An Edge Native Platform for Edge and Network Security

Intel® Smart Edge: Flexible Adoption Models

For App Developers, Edge Builders and Enterprise Buyers

Smart Edge Building Blocks

SaaS Layer	5G RAN
	5G Core
	SDWAN
	Firewall
	Apps
PaaS layer	Zero Trust Security Service
	Networking Service
	Observability Service
	Dataplane Service
	Service Mesh
	Accelerator Service
	Storage Service
	Registry Service
	App LCM Service
	5G RAN Service
	5G Core Service
	SASE Service
	Analytics Service
	Green Edge Service
	Multi-tenancy Service
CaaS layer	Container Orchestration Service
	Container Runtime Service
	Virtual Machine Service
IaaS layer	Operating System Service
	Provisioning Service
	Platform Service

Assemble → Optimize → Integrate → Deploy

Pre-Integrated and Optimized for the Edge

- Pre-built optimizations on Intel® architecture for your edge platform
- Faster path to market with tailored offerings that are pre-validated

Intel® Smart Edge for Developers

App Developers: **Develop** with us

Application SDKs for building Edge Native applications

Intel® Smart Edge for Builders

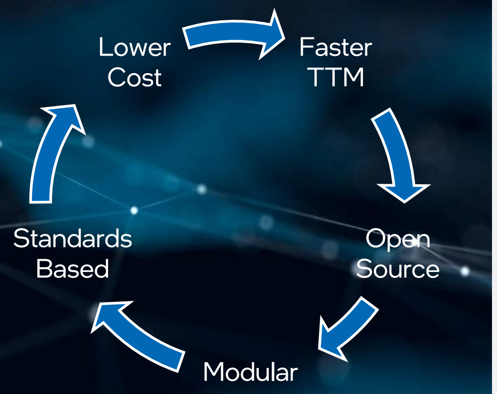
Solution Providers: **Build** with us

Optimized and Integrated for Edge Services and Locations

Intel® Smart Edge for Enterprises

Select Enterprise Users: **Buy** with us

With UI, Orchestration & Management tools



Intel® Smart Edge Open Secure Access Service Edge Experience Kit

On Premises Edge

Edge Deployment of intelligent sensors and gateways at Industrial, Retail or Enterprise locations

Industrial

Healthcare

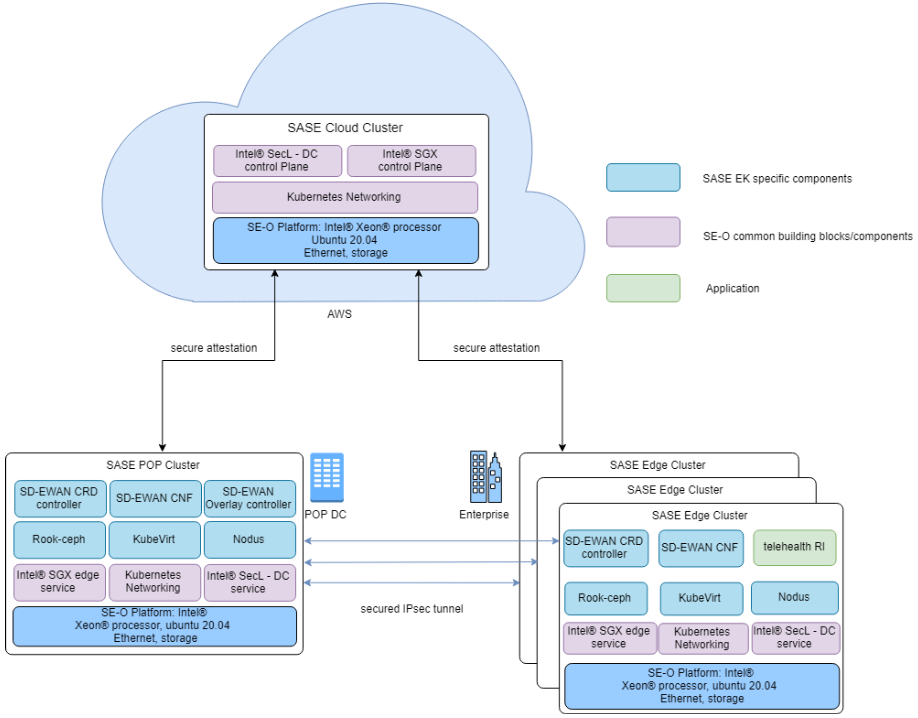
Retail

What does it do?

- The **Secure Access Service Edge Experience Kit** provides a blueprint for a SASE Edge and POP configuration for deploying Containerized Network Functions and legacy VNFs for SASE and SSE with platform and network security

What does it have?

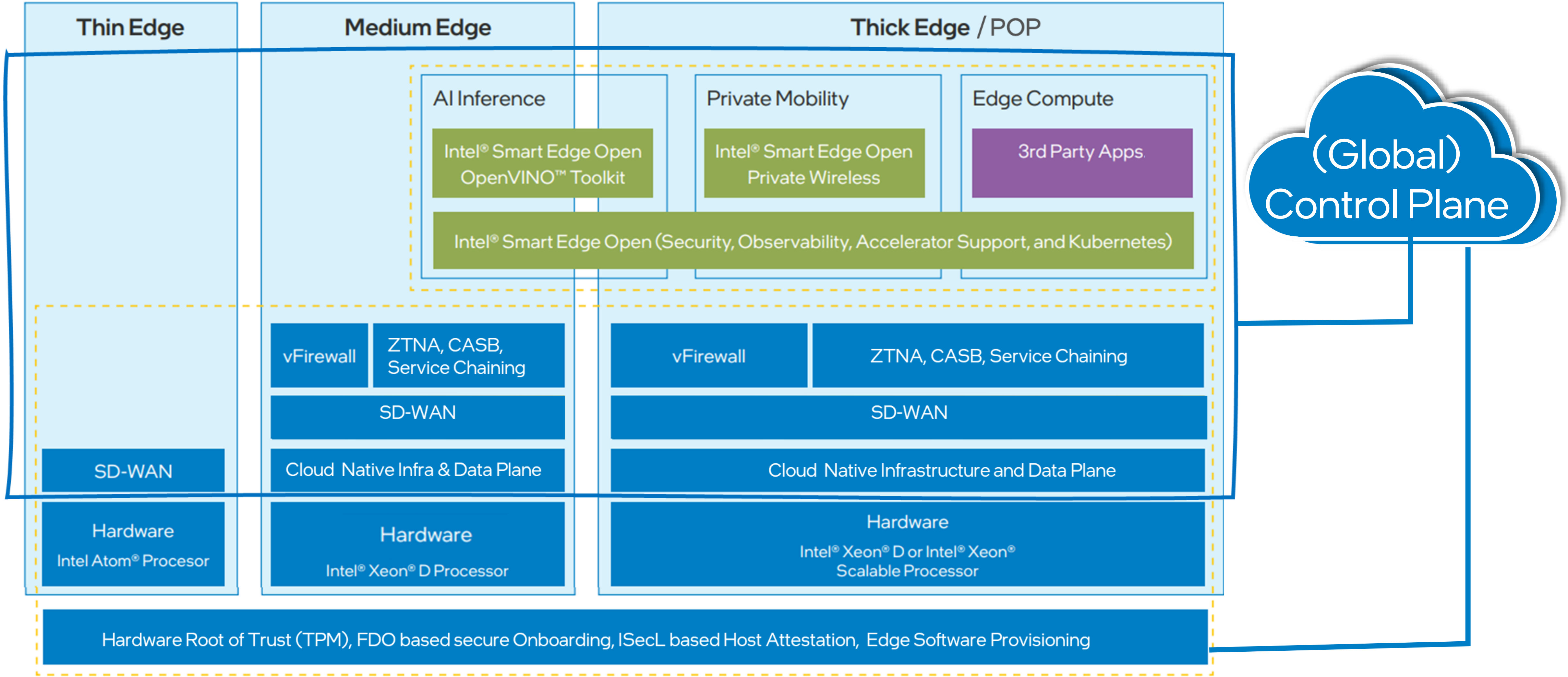
- Container Orchestration Service
- Data Plane & Networking service
- Observability service
- Analytics service
- Storage service
- Zero Trust Edge Compute Protection
- Platform and Provisioning service
- SASE service



Use Cases

- Threat prevention, web filtering, sandboxing, DNS security, credential theft prevention, data loss prevention and next-generation firewall policies

SASE for Enterprise Edge and POP


Thin Edge
Medium Edge
Thick Edge / POP
AI Inference
Intel® Smart Edge Open OpenVINO™ Toolkit
Private Mobility
Intel® Smart Edge Open Private Wireless
Edge Compute
3rd Party Apps
Intel® Smart Edge Open (Security, Observability, Accelerator Support, and Kubernetes)
vFirewall
ZTNA, CASB, Service Chaining
vFirewall
ZTNA, CASB, Service Chaining
SD-WAN
SD-WAN
SD-WAN
Cloud Native Infra & Data Plane
Cloud Native Infrastructure and Data Plane
Hardware
Intel Atom® Procesor
Hardware
Intel® Xeon® D Processor
Hardware
Intel® Xeon® D or Intel® Xeon® Scalable Processor
Hardware Root of Trust (TPM), FDO based secure Onboarding, ISecL based Host Attestation, Edge Software Provisioning
(Global) Control Plane

References

Software Reliability

- Extended Page Tables Sub-page Write Protection (EPT-SPP)
- Intel® Control-Flow Enforcement Technology (Intel® CET)
- Intel® Threat Detection Technology (Intel® TDT)
- Anomalous Behavior Detection for Intel® TDT
- Page Protection Keys
- User-Mode Instruction Prevention (UMIP)

Workload and Data Protection

- Advanced Programmable Interrupt Controller Virtualization (APICv)
- Intel® OS Guard
- Intel® Secure Key
- Intel® Software Guard Extensions (Intel® SGX)
- Intel® Virtualization Technology (Intel® VT)
- Intel Virtualization Technology - Redirect Protection (Intel® VT-rp)
- Mode-Based Execution Control

Foundational Security

- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
- Intel® Crypto Acceleration
- Intel® BIOS Guard
- Intel® Boot Guard
- Intel® Converged Security and Management Engine (Intel® CSME)
- Intel® Firmware Guard
- Intel® Platform Firmware Resilience (Intel® PFR)
- Intel® Platform Trust Technology (Intel® PTT)
- Intel® QuickAssist Technology (Intel® QAT)
- Intel® Runtime BIOS Resilience
- Intel® System Resources Defense
- Intel® System Security Report
- Intel® Total Memory Encryption (Intel® TME)
- Intel® Total Memory Encryption – Multi-Key (Intel® TME-MK)
- Tunable Replica Circuit - Fault Injection Detection
- Intel® Trusted Execution Technology (Intel® TXT)

https://intel.com/securityinnovations

References

1. Intel® Smart Edge
   - https://www.intel.com/content/www/us/en/edge-computing/smart-edge.html
   - https://smart-edge-open.github.io/docs/product-overview
2. Intel Security Innovations https://intel.com/securityinnovations
3. A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted Internet of Things," IEEE Internet Things J., vol. 8, no. 6, pp. 4004–4022
4. Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu and W. Lv, "Edge Computing Security: State of the Art and Challenges", Proc. IEEE, vol. 107, pp. 1608-1631, 2019

intel®