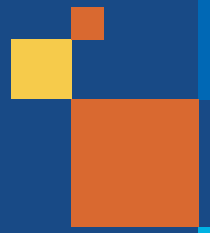
Rethink Zero Trust with Confidential Computing Technologies and In Service Mesh

Xiang Wang (xiang.w.wang@intel.com)

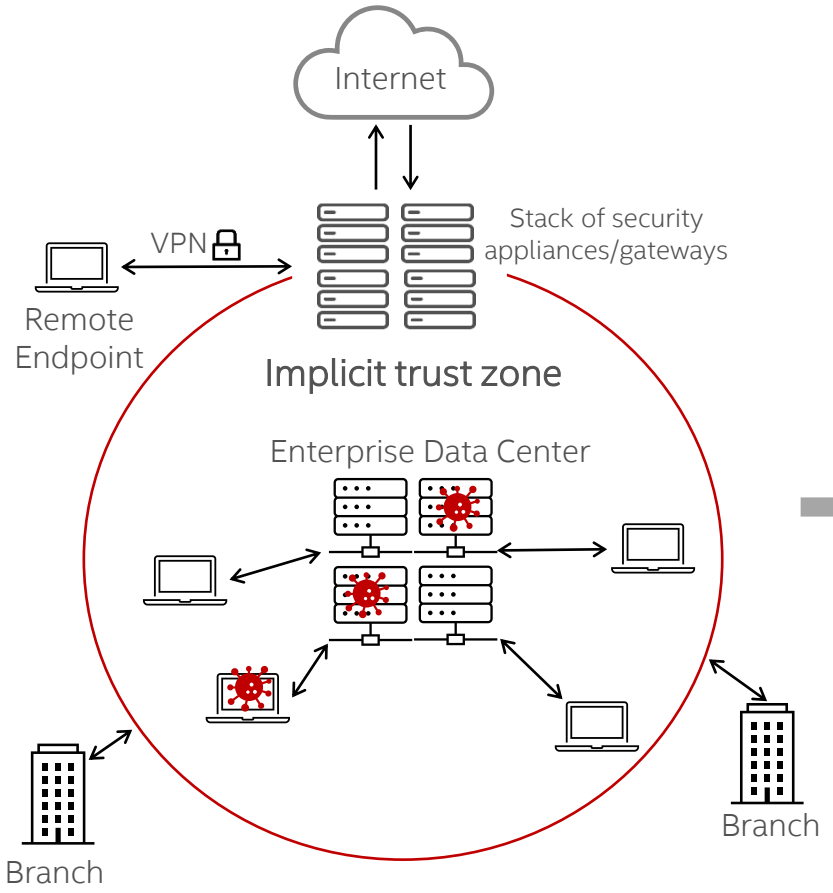


intel®

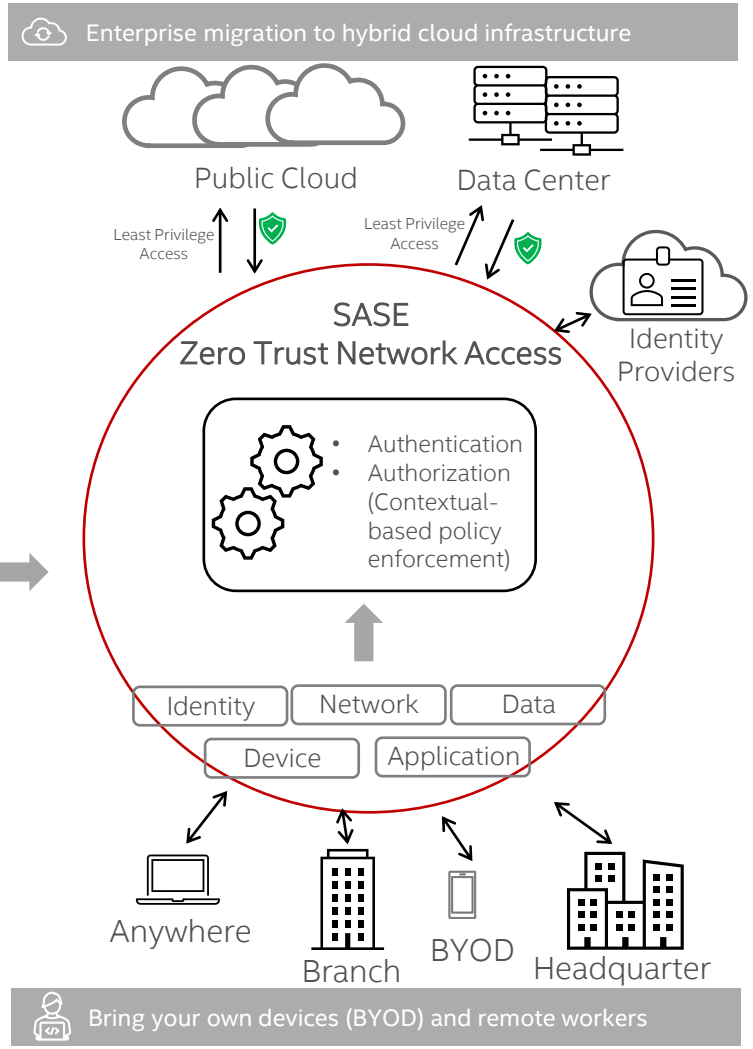
Agenda

- Introduction to Zero Trust
- Zero Trust Service Mesh
- Intel Zero Trust Reference Architecture

Zero Trust is Critical



Legacy castle-and-moat network model



Zero Trust Network Access model

Gartner

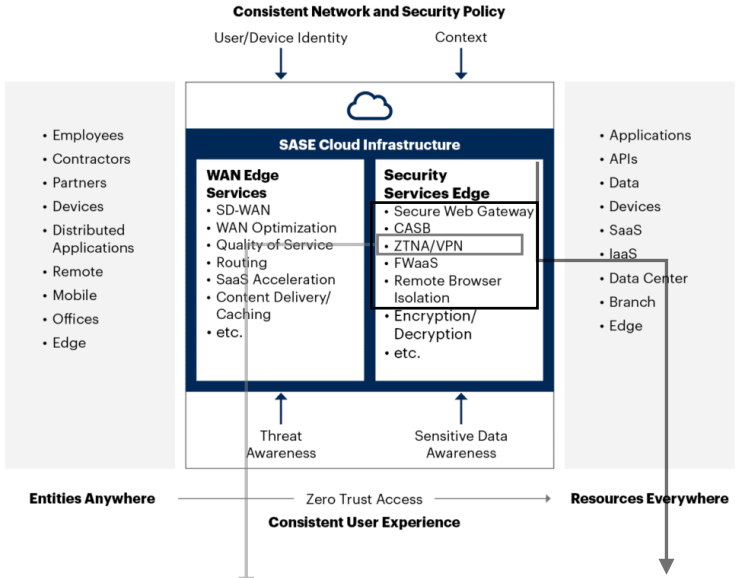
80% of new digital business applications will be accessed through ZTNA.

60% of enterprises will phase out most of their remote access VPNs in favor of ZTNA.

60% YoY growth rate for ZTNA from 2019 to 2025.

Federal Government

Mandates the move toward Zero Trust Strategy.



Zero Trust is a core component of SASE

Fully integrated SSE platform

Zero Trust Is Challenging

Least Privilege	Service Authorization	Preventing Lateral Movement	Secure Communication	
Microsegmentation	Identity and Device Authentication	Context-based Monitoring	Multi-factor Authentication	

Secrets Are Hard to Protect

- Secrets (passwords, tokens, encryption keys, certificates, etc) are everywhere.
- Protect secrets at rest, in transit and in use.

Encrypted Network Tunnels Are Expensive

- Every communication channel must be encrypted (clients to SASE, SASE to cloud services).
- Asymmetric and symmetric crypto are compute intensive.

Access Controls Are Complex

- A myriad of policy rules.
- Role-based access control (RABC) is heavy.

Intel Values -> Zero Trust – Intel® SGX

Traditional encryption is proven and trusted, but there are gaps

Data at rest

Encrypt data in storage, database, etc

Data in transit

Encrypt data in network flows

Data in use encryption – Intel SGX

Data in use

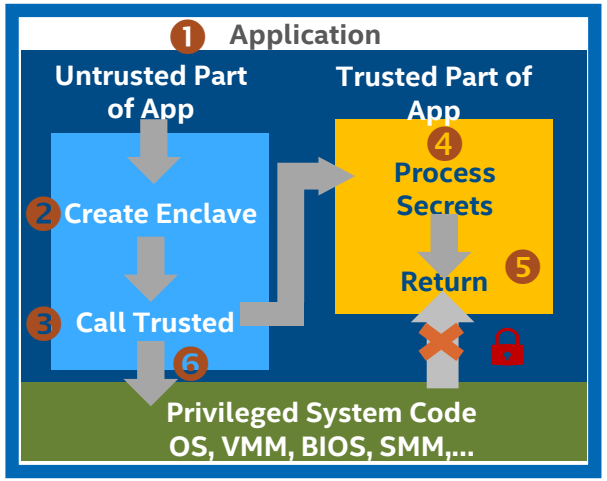
Encrypt data in use/computation, while in RAM

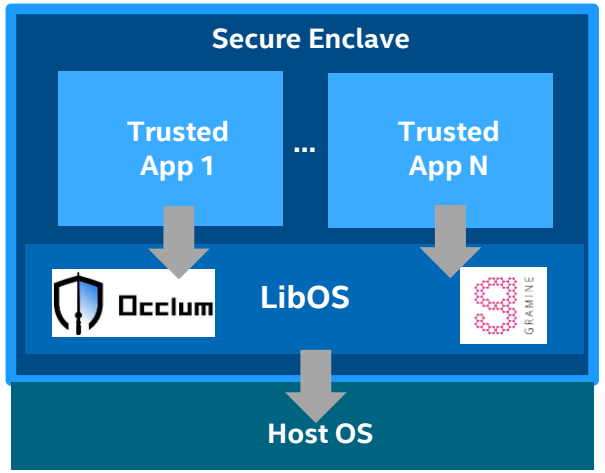
- **Secrets management**
- **Public cloud security/compliance**
- **Blockchain**
- **Multi-party computing**

Intel SGX (Intel® Secure Guard Extensions):

- Protects sensitive data in secure enclave even in the presence of privileged code at the OS, BIOS, VMM, or SMM layers
- Deployment models:
  - Purpose built application with untrusted and trusted part using SGX SDKs
  - Direct deployment with LibOS (Occlum/Gramine)
- Supported platforms:
  - 3rd Gen Intel® Xeon® Scalable processors and Intel® Xeon® D-2700/D-1700 processors

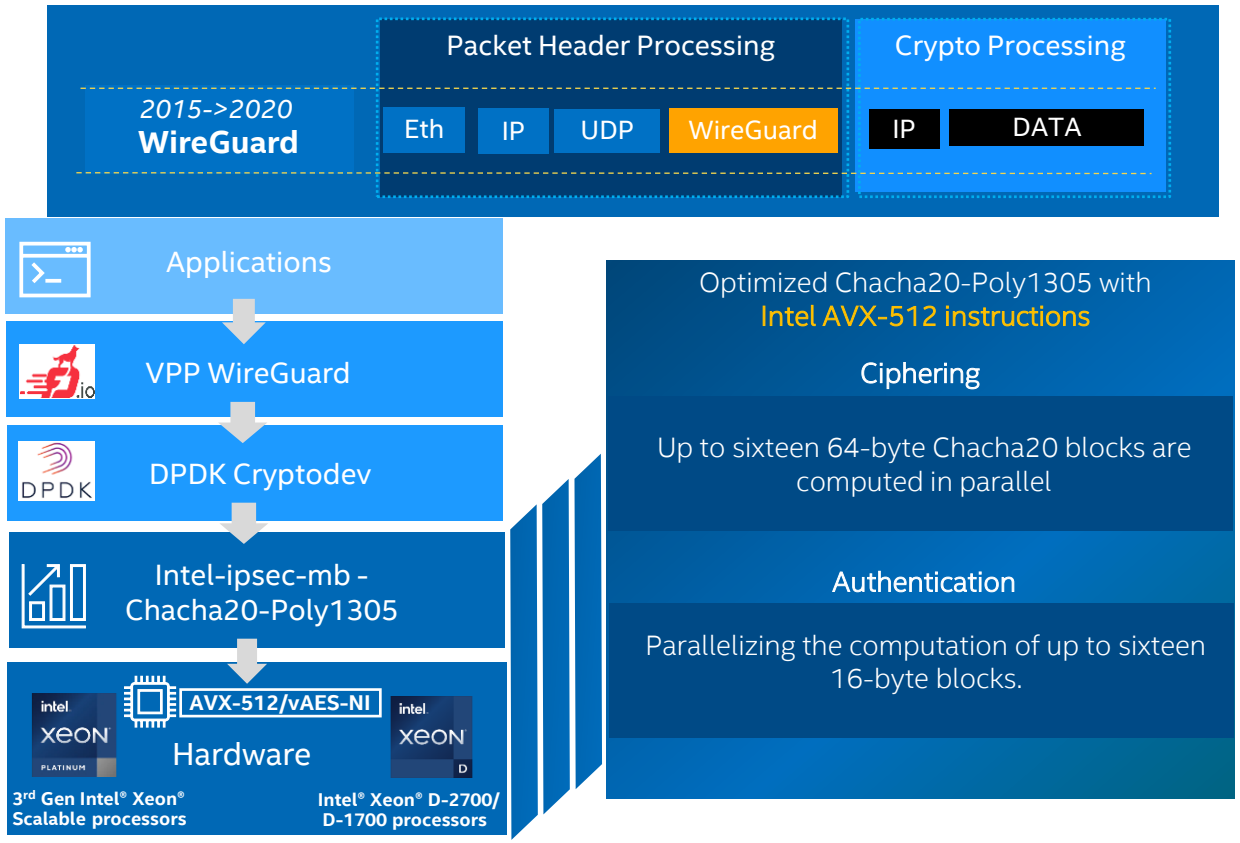
Intel SGX deployment models

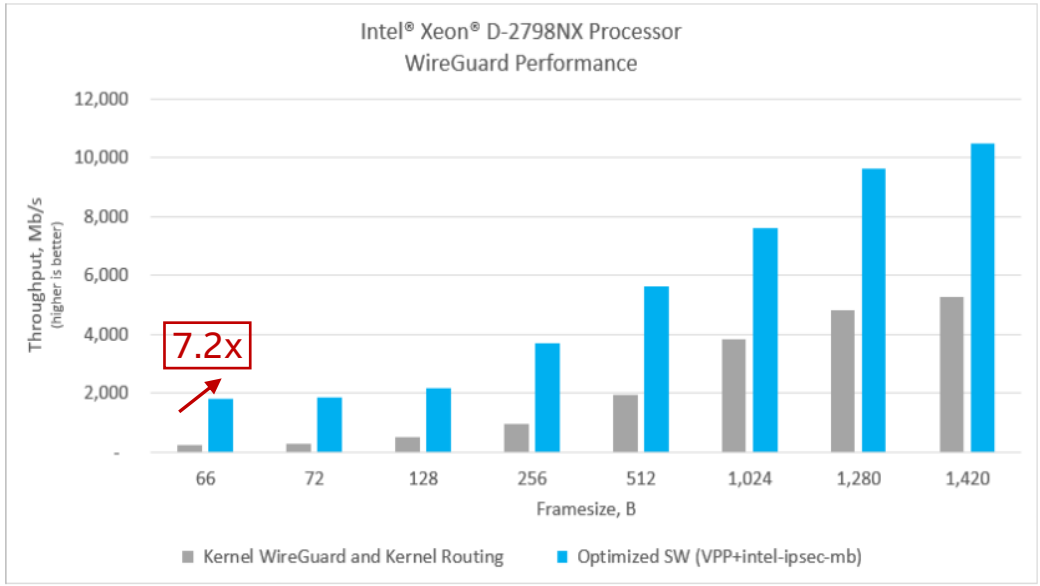




Intel SGX protects secrets (passwords, tokens, encryption keys, etc) in zero trust

Intel Values -> Zero Trust - WireGuard Acceleration





WireGuard encryption and decryption for various packet sizes:
- Linux Kernel WireGuard
- VPP WireGuard encryption and decryption both using the intel-ipsec-mb library to process Chacha20-Poly1305 cryptographic processing

Intel processors boost WireGuard tunnel performance significantly in zero trust

Fast Multi-buffer IPsec Implementations on Intel® Architecture Processors- Link
Accelerate WireGuard Processing with Intel® Xeon® D-2700 Processor Technology Guide – Link

Zero Trust Service Mesh

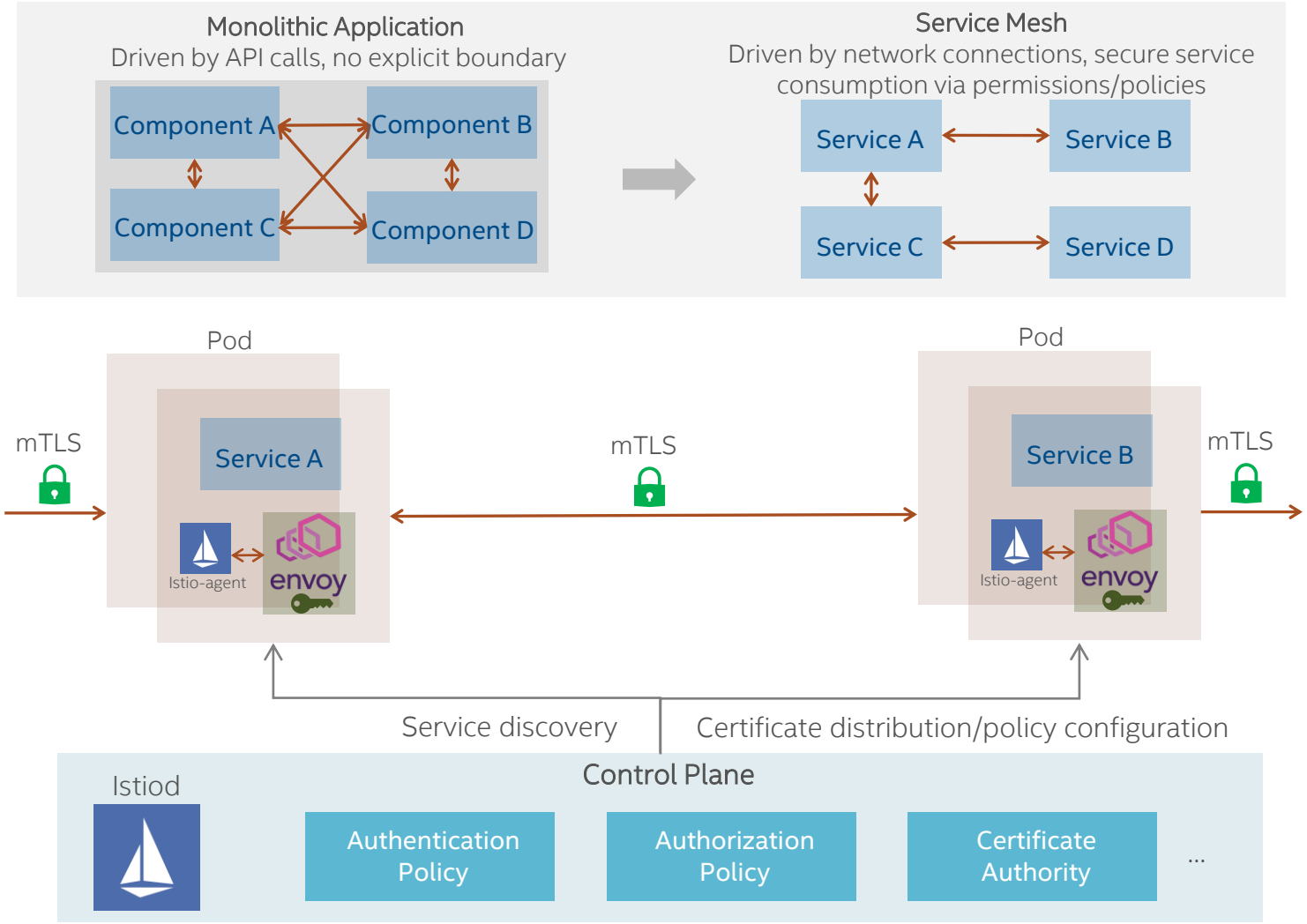
Zero Trust Service Mesh

Zero trust for service mesh: Istio, HashiCorp Consul, Kong…

1) Services is authenticated and encrypted using mutual TLS (mTLS).

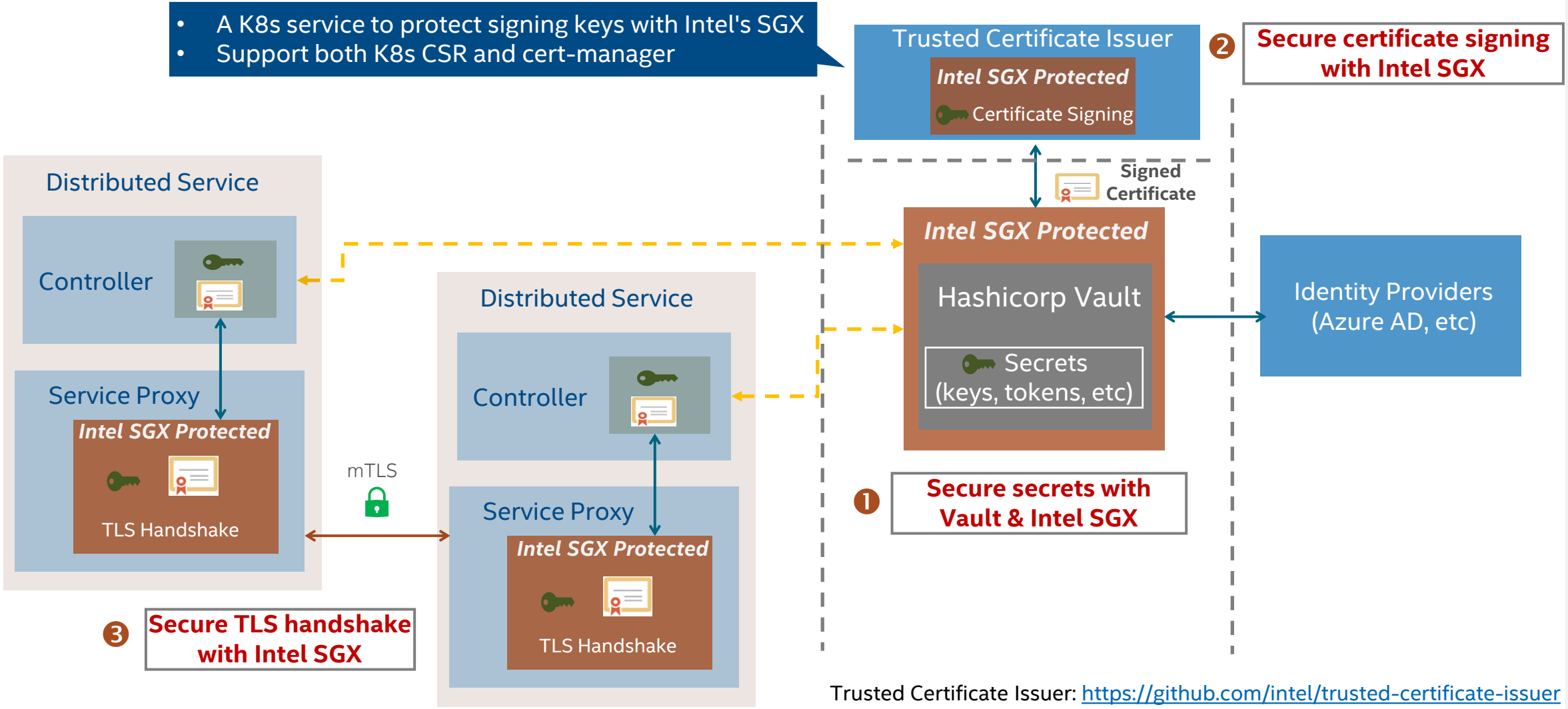
2) Authorization policies for inter-service communications

```
apiVersion: "rbac.istio.io/v1alpha1"
kind: ServiceRole
metadata:
  name: products-viewer
  namespace: default
spec:
  rules:
  - services: ["products.default.svc.cluster.local"]
    methods: ["GET", "HEAD"]
```



Zero Trust Service Mesh with Confidential Computing

- A K8s service to protect signing keys with Intel's SGX
- Support both K8s CSR and cert-manager

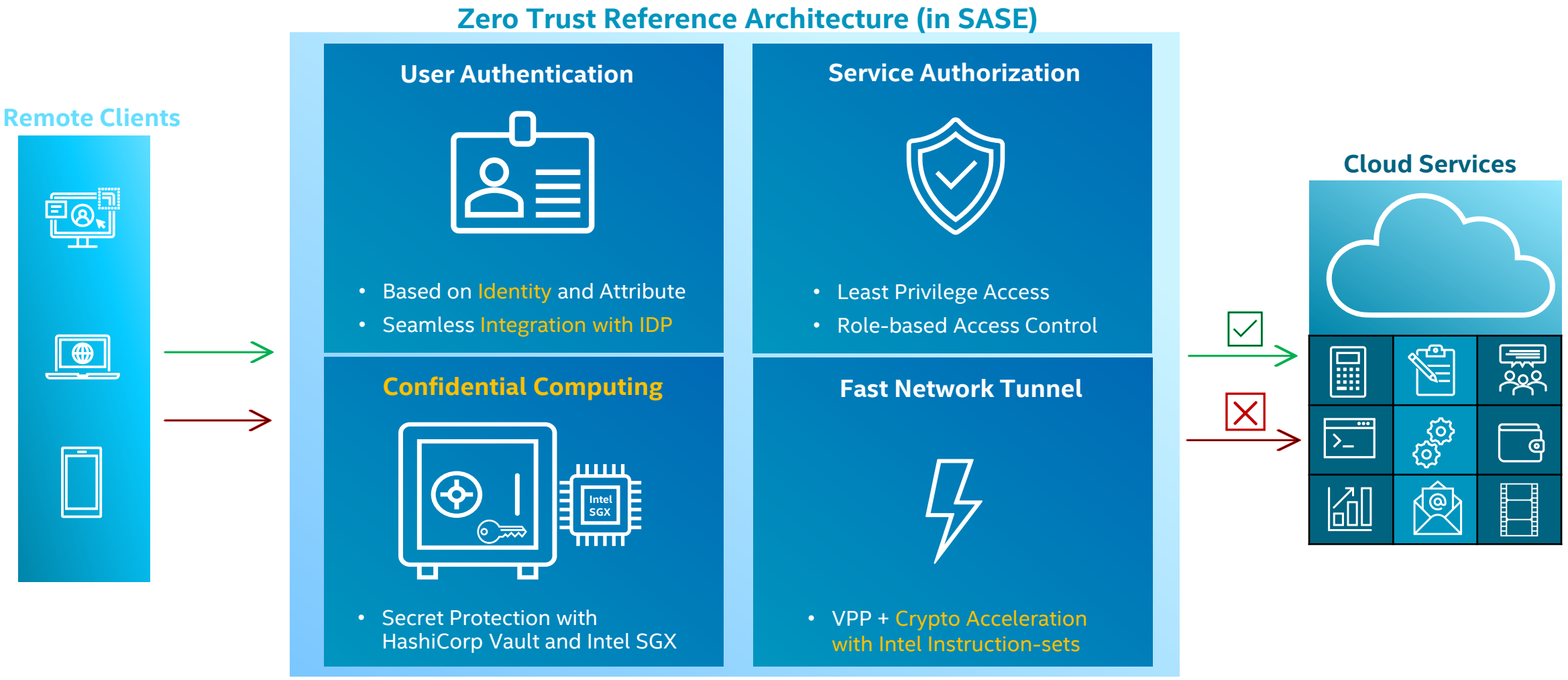


Trusted Certificate Issuer: https://github.com/intel/trusted-certificate-issuer

Intel Zero Trust Reference Architecture

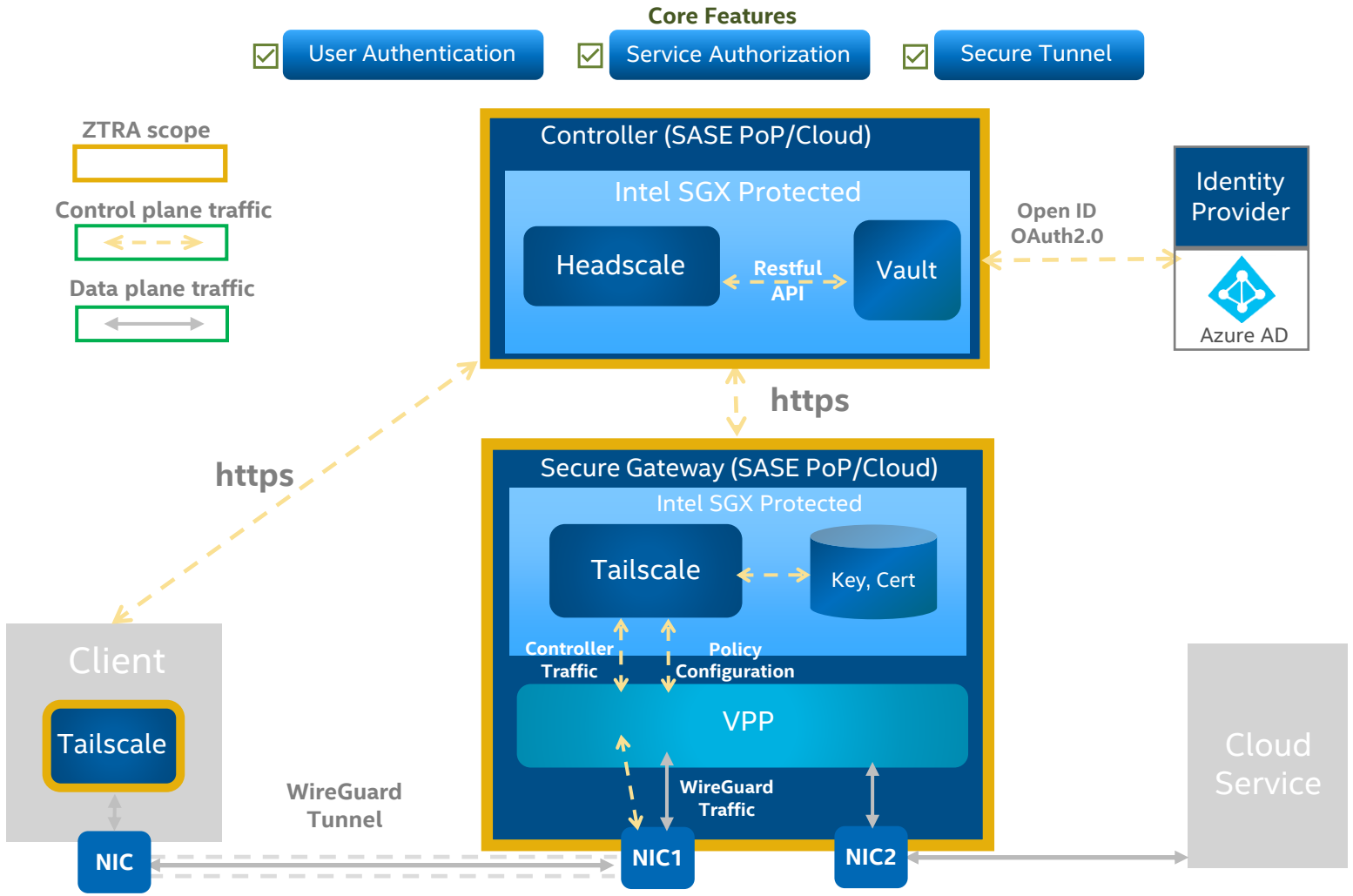
Zero Trust Reference Architecture (ZTRA)

Rethink Zero Trust Software (IPL) with latest Intel Platforms



Zero Trust Reference Architecture Overview

A multi-node and end-to-end system deployment



Software package

- Intel Proprietary License (IPL)
- Include Controller and Secure Gateway
- Client (Tailscale) not included – self deployment

Controller

Features

- User authentication with Headscale & Azure Active Directory
- Role Based Access Control (RBAC)
- Secrets management with HashiCorp Vault
- Secrets protection in SGX enclave

Platform

3rd Gen Intel® Xeon® Scalable processors

Intel® Xeon® D-2700/ D-1700 processors

Secure Gateway

Features

- VPP WireGuard tunnel w/ AVX-512
- Service authorization w/ VPP ACL
- Key protection in Intel SGX enclave
- VPP integration with Tailscale

Platform

3rd Gen Intel® Xeon® Scalable processors

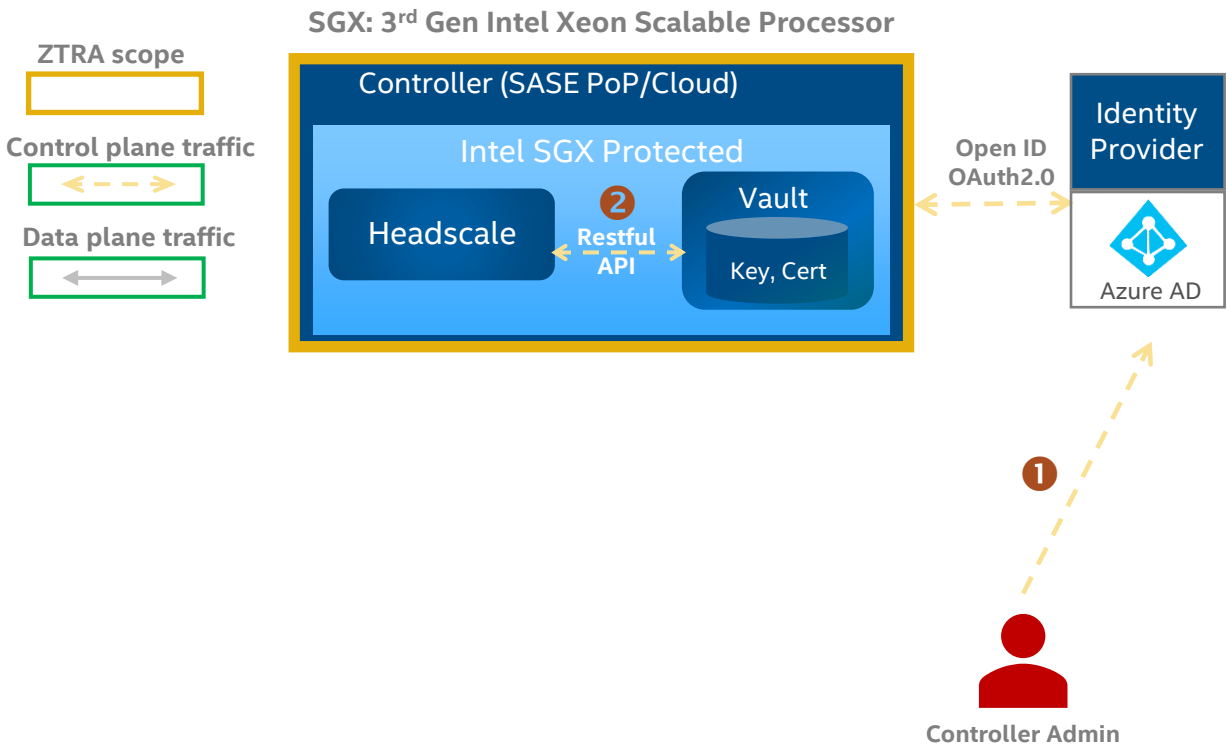
Intel® Xeon® D-2700/ D-1700 processors

User Authentication(1)

Controller APP Registration:

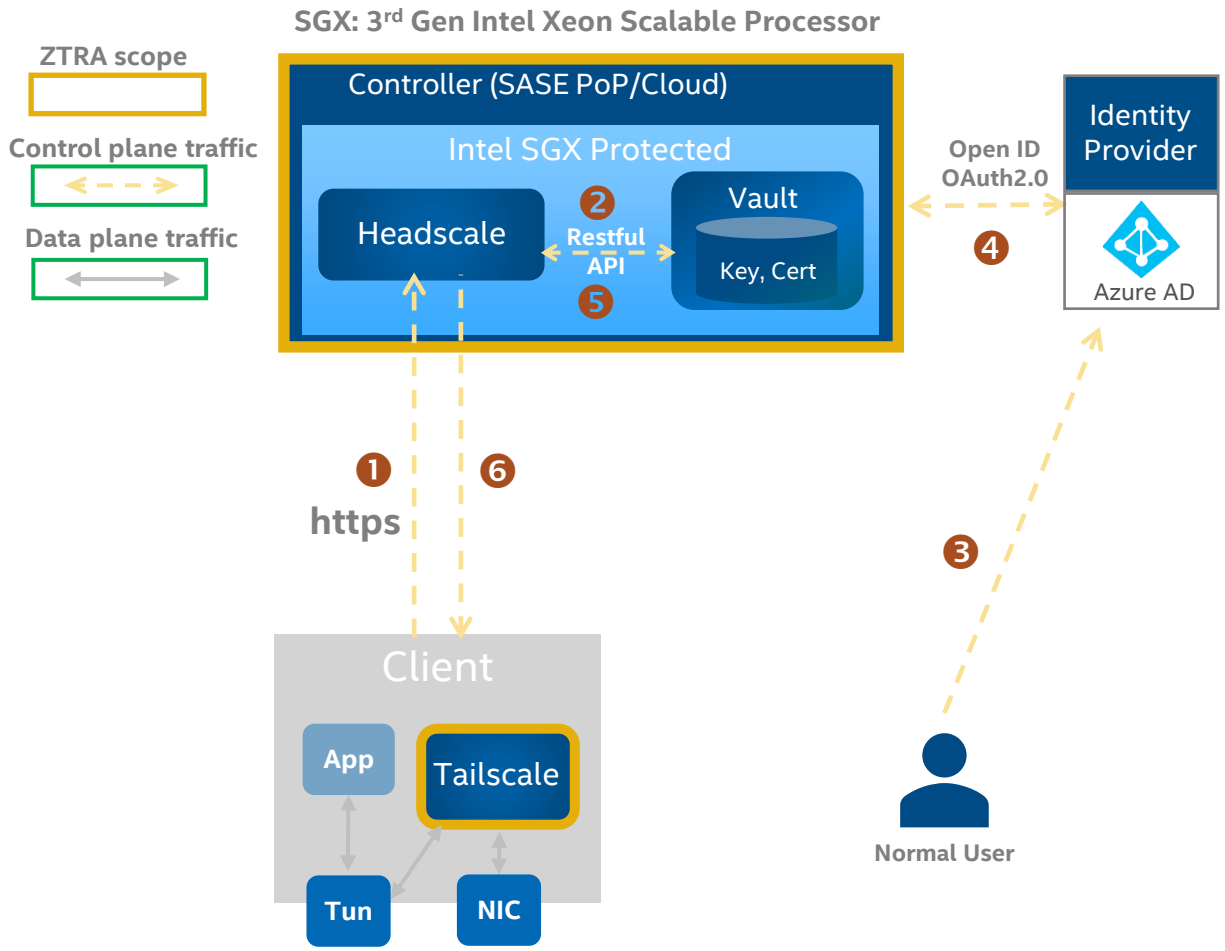
1) Controller admin registers an APP account with an IDP.

2) Controller configures APPID, APPSecret, tokenURL, authURL, redirectURL, etc in Vault.



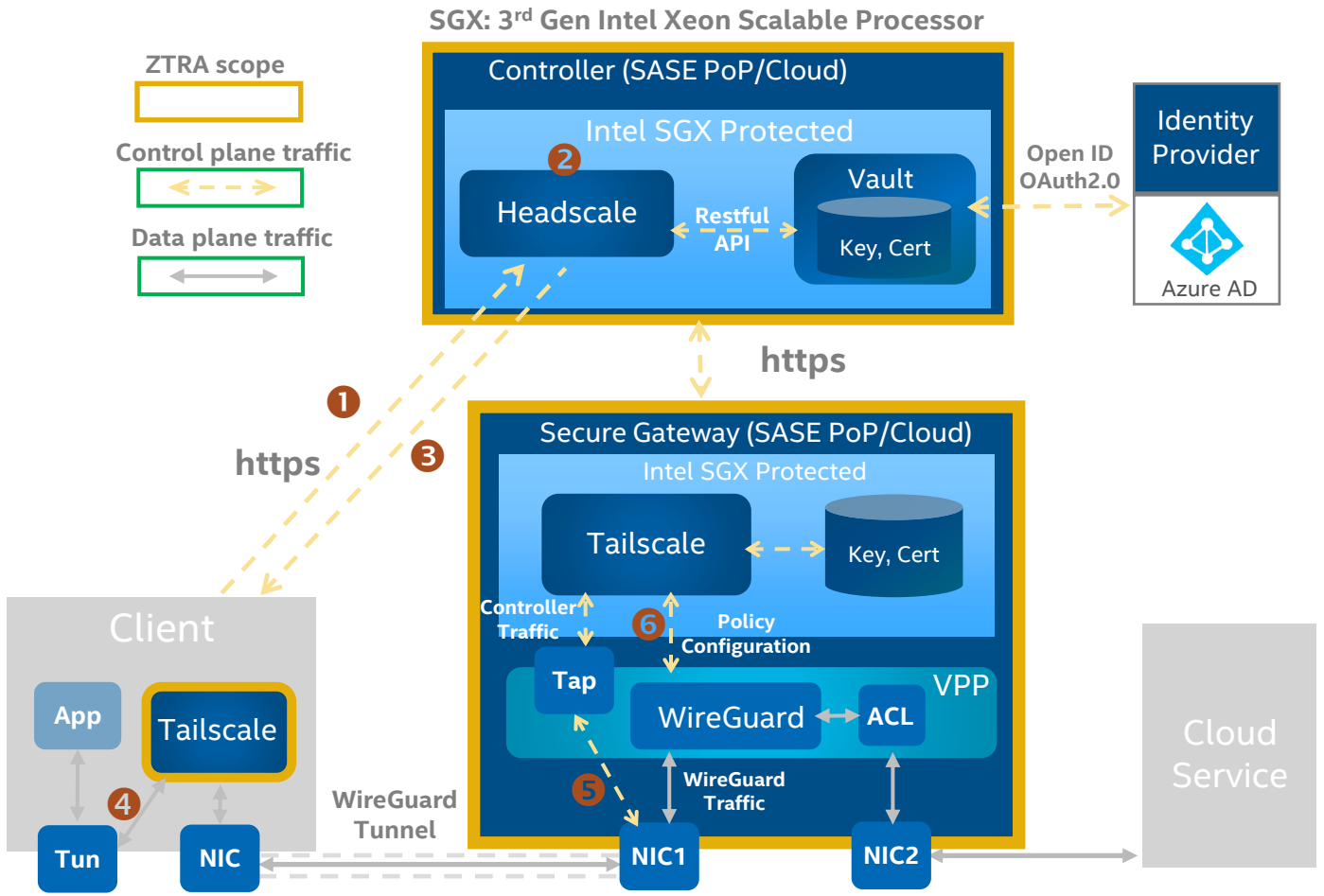
User Authentication(2)

1) Client sends authentication request with machine public key.
2) Vault generates an authorization URL (https://authurl?redirect_uri=http://redirect_ip:redirect_port/odic/callback&scope=xxx&response_type=code &state=xxx&appid=xxx.).
3) User visits the authorization URL, provides identity info and approves the authorization.
4) Vault receives the OIDC callback and visits authorization endpoint (https://tokeurl?code=xxx&appid=xxx&appsecret=xxx& grant_type=authorization_code) to get access token.
5) Headscale receives access token from Vault and saves client node as registered.
6) Client receives successful authentication response.



Service Authorization(1)

1) Client sends an authorization request to Controller.
2) Controller checks Client identity (with public key) and generates ACL rules.
3) Controller returns assigned IP, peer info, etc in the response for a valid Client.
4) Client configures TUN interface with IP, routes, etc.
5) Controller passes control messages (peer info, ACL, etc) to Secure Gateway via a TAP interface in VPP.
6) Secure Gateway configures ACL in VPP.



Service Authorization(2)

- Role Based Access Control (RBAC):
  - Group: a cluster of users, hostname, namespace, etc.
  - Tag: attribute assigned to client device.
- Controller decodes and distributes ACL rules to data plane as srcIP&dstIP&port&proto.
- Secure gateway keeps a long live connection with Controller. ACL updates at Controller will reflect to data plane.

```
{
  "acls": [
    {
      "action": "accept",
      "src": ["tag:webdevice", "group:sre"],
      "dst": ["tag:webserver"]
    }
    // Other access rules here...
  ]
  // Other policy configuration here...
}
```

Data Plane Workflow

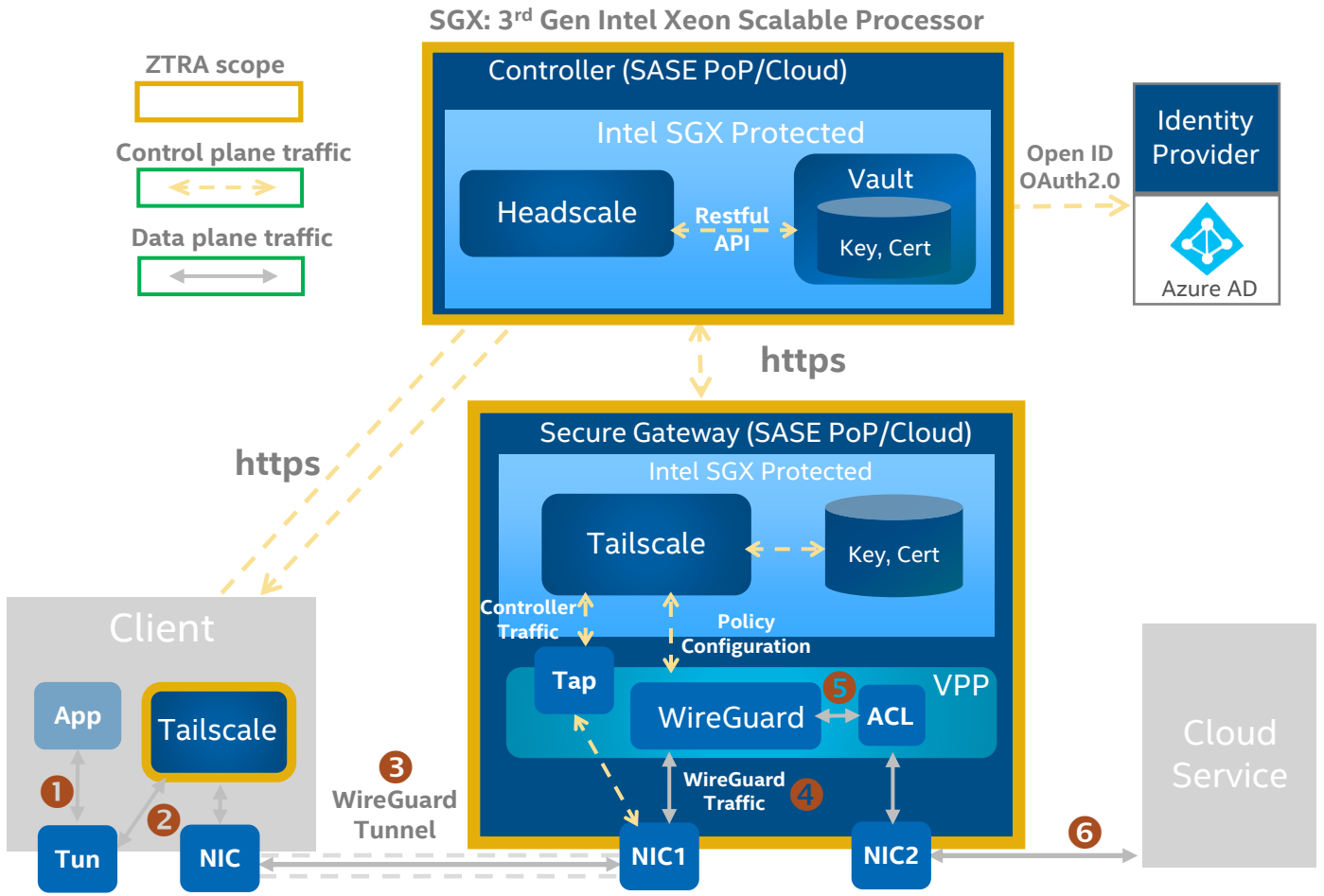
- Service request data path:

  In client device:

  1) Endpoint app sends a service request via a configured TUN device.
  2) TUN device forwards the traffic to Tailscale.
  3) Tailscale sends the request to Secure Gateway by establishing a WireGuard tunnel.

  In Secure Gateway:

  4) VPP WireGuard plugin (accelerated by AVX512) receives the traffic from endpoint.
  5) VPP enforces ACL policy for service authorization.
  6) VPP forwards the traffic to remote service if granted.



ZTRA – What to Expect

ZTRA 22.06 **(Released)**

User Authentication

Service Authorization

Vault Integration
- Secret management
- IDP Integration

Intel SGX Support

VPP Integration:
- WireGuard Tunnel
- ACL Matching

New Features in planning

Cloud Deployment on Azure
- Build a cloud demo

IPsec Support

Full Disk Encryption

Let's Encrypt Integration

...

Get Started

- ZTRA 22.06 software package access
  - Register account for Intel RDC (link)
  - Free source code download with approved Software License agreement from Intel (Intel Proprietary License) (link)
- Contact Intel Representative
  - Xiang Wang (xiang.w.wang@intel.com)
  - Heqing Zhu (heqing.zhu@intel.com)


intel

Notices and Disclaimers

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

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

No product or component can be absolutely secure.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Notices and Disclaimers

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

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

No product or component can be absolutely secure.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.