Grid Cyber Security Component Allocation Examples

1.2.1 GMLC Grid Architecture Project

Grid Security Measures Functional Categories

Access Control

- User and Device Identity
- Authentication, Authorization & Accounting

Data Integrity, Confidentiality and Data Privacy

- Network Segmentation
- Security Connectivity and Encryption (VPN)

Threat Detection and Mitigation

- Security Zones with Firewall
- Intrusion Prevention with SCADA signatures

Device and Platform Integrity

- Device Hardening
- Configuration Assurance

Legend

- Secure Device Identity Via X.509 Certificates
- Strong User Identities With Role-Based Access
- Mutual Authentication, Authorization and Accounting for Each User and Device

- Secure Storage for Encryption Keys
- Secure Encryption Keys (Mesh)
- Mesh With Link-layer Encryption

- Secure Storage for Encryption Keys
- Secure Encryption Keys
- Links With Network-Layer Encryption

- Secure Storage of Encryption Keys
- Secure Encryption Keys
- Application Layer Encryption

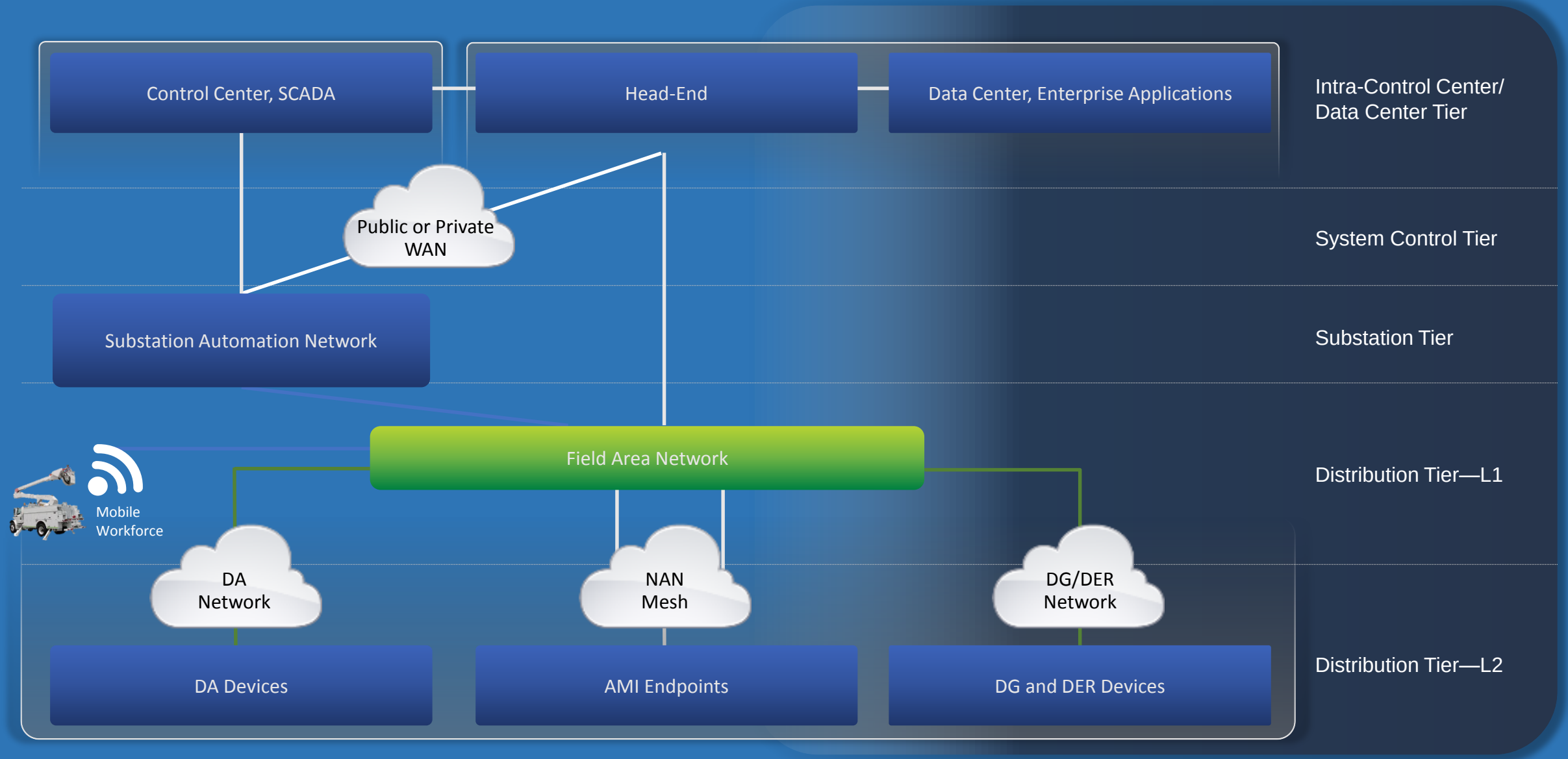
- Network Segmentation of Users and Devices
- Data Separation Over Shared Links
- Firewalls and Access Control

- Time-stamped Logs Across Devices
- IPS With SCADA Signatures
- Security Incident Reporting Through Log Correlation and IPS Alerts

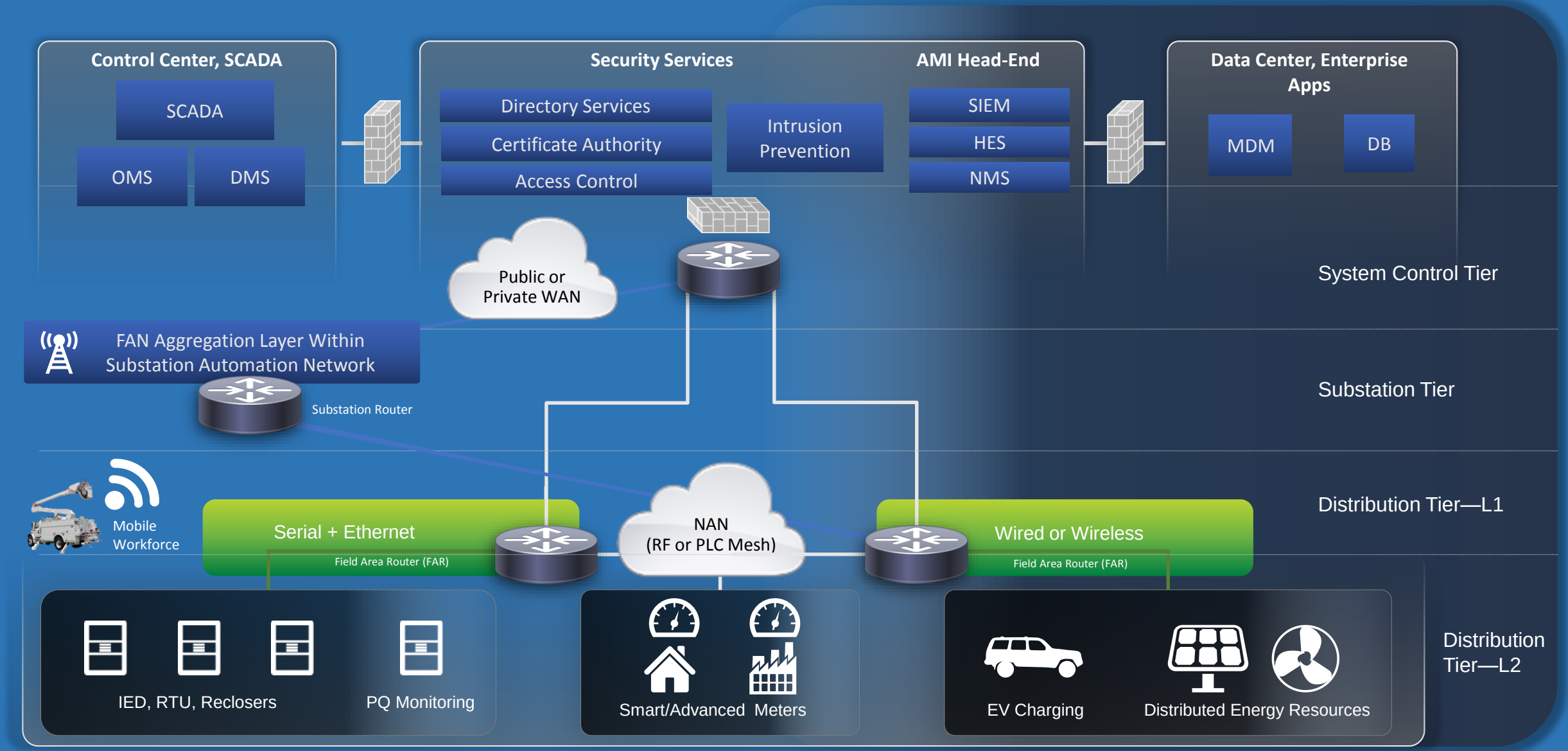
- Anti-virus and Anti-malware Protection
- Posture Assessment and Remediation (Patch Management)
- Network Admission Control
- Electronic security perimeter

Field Area Networks

Field Area Network



Field Area Network



Access Control

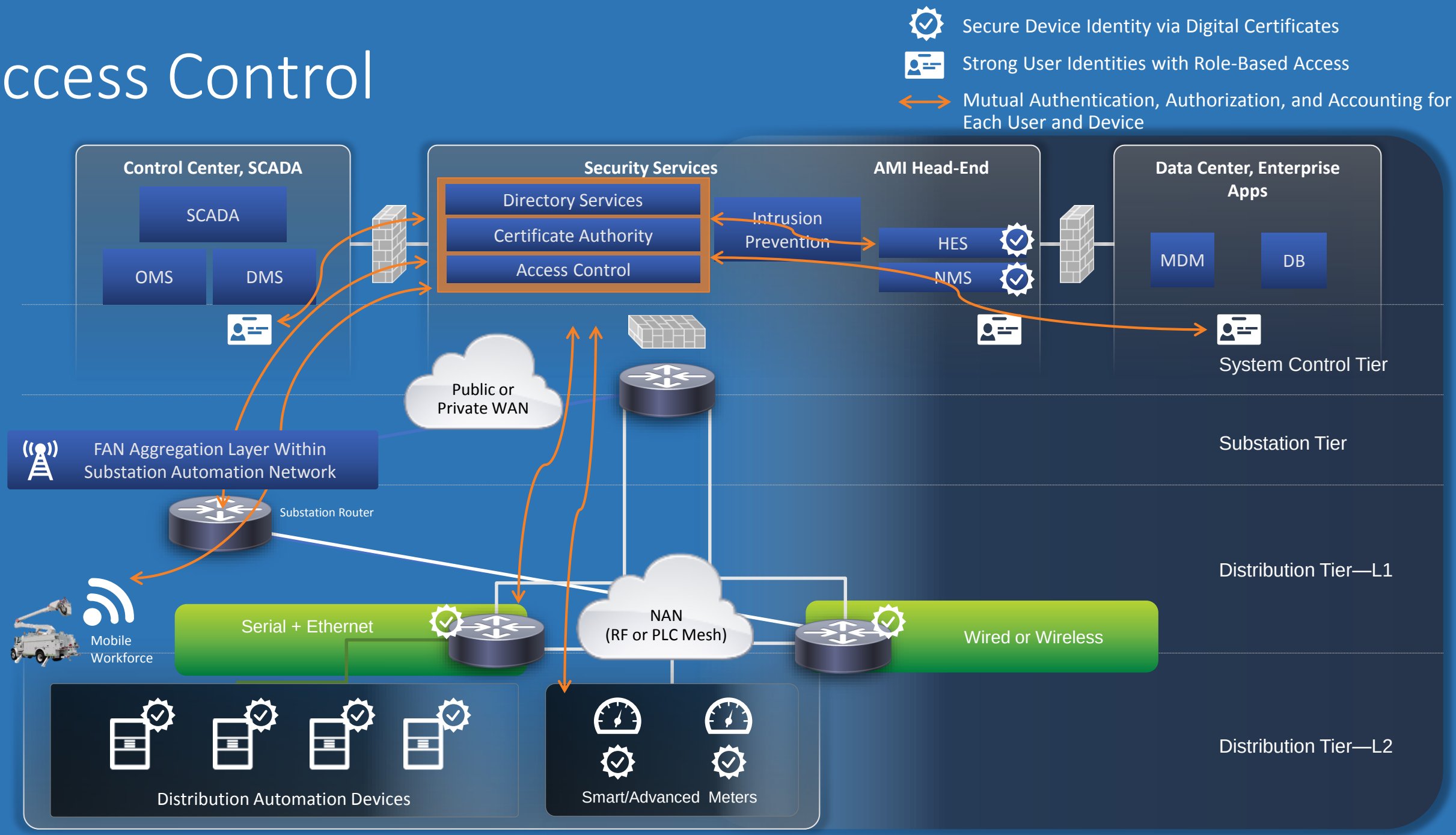
Purpose: Ensure that only authorized personnel are accessing the network and valid devices are part of the grid network

Components: Role-Based Access Control with i) username and passwords ii) X.509 certificate based identities; RADIUS and TACACS+ protocols for Authentication, Authorization and Accounting (AAA) for users and devices; Network Admission Control (NAC)

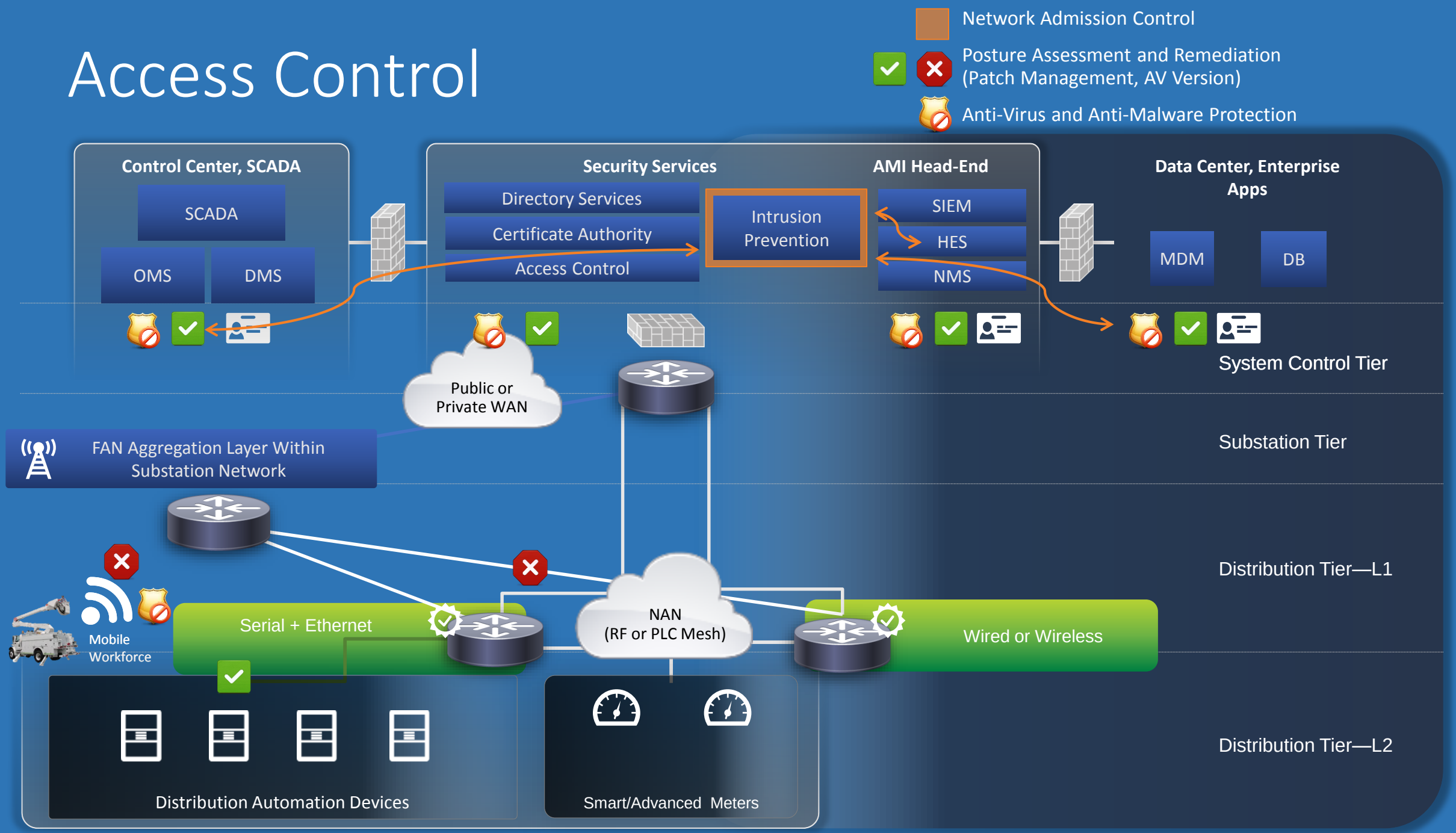
Used in FAN and AMI for:

- Authenticating and authorizing field technicians or operations center staff before they can view or configure devices, track changes made (RBAC)
- Authenticating every device and application connected to the grid—routers, switches, servers, workstations, IEDs, reclosers
- Mutually authenticating meters, field area routers and head-end systems used for smart metering—relying on strong certificate based identities
- Posture-assessing laptops, workstations, servers to detect any viruses or worms before allowing access to the network, forcing remediation such as installing software patches or updating anti-virus database

Access Control



Access Control



Data Confidentiality and Privacy

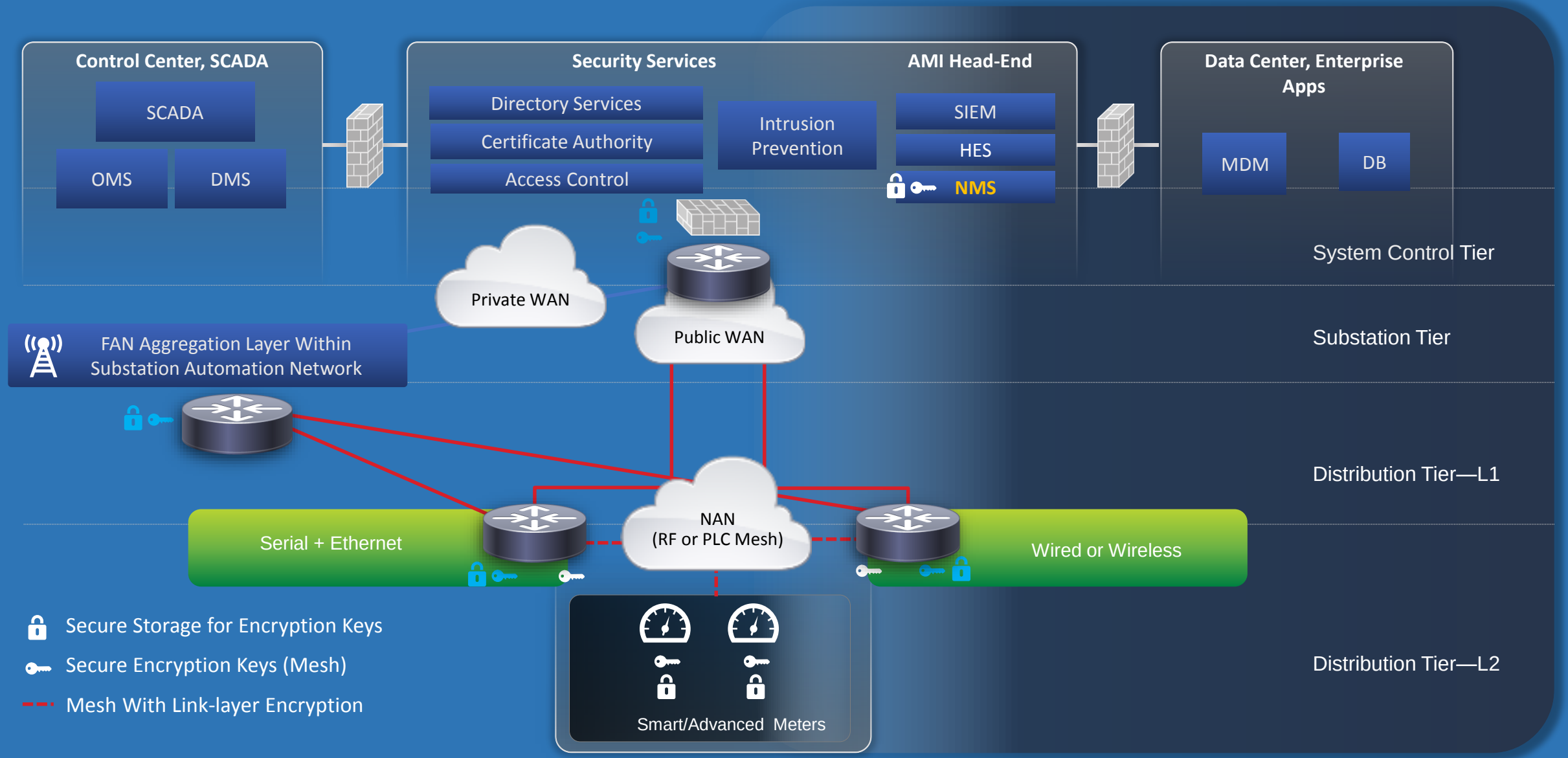
Purpose: Ensure data privacy and data integrity for customer data and data integrity and confidentiality for technical data belonging to the utility

Components: X.509 Certificate, IPSec with flexible VPN architectures, link-layer and application layer encryption mechanisms, scalable crypto key management

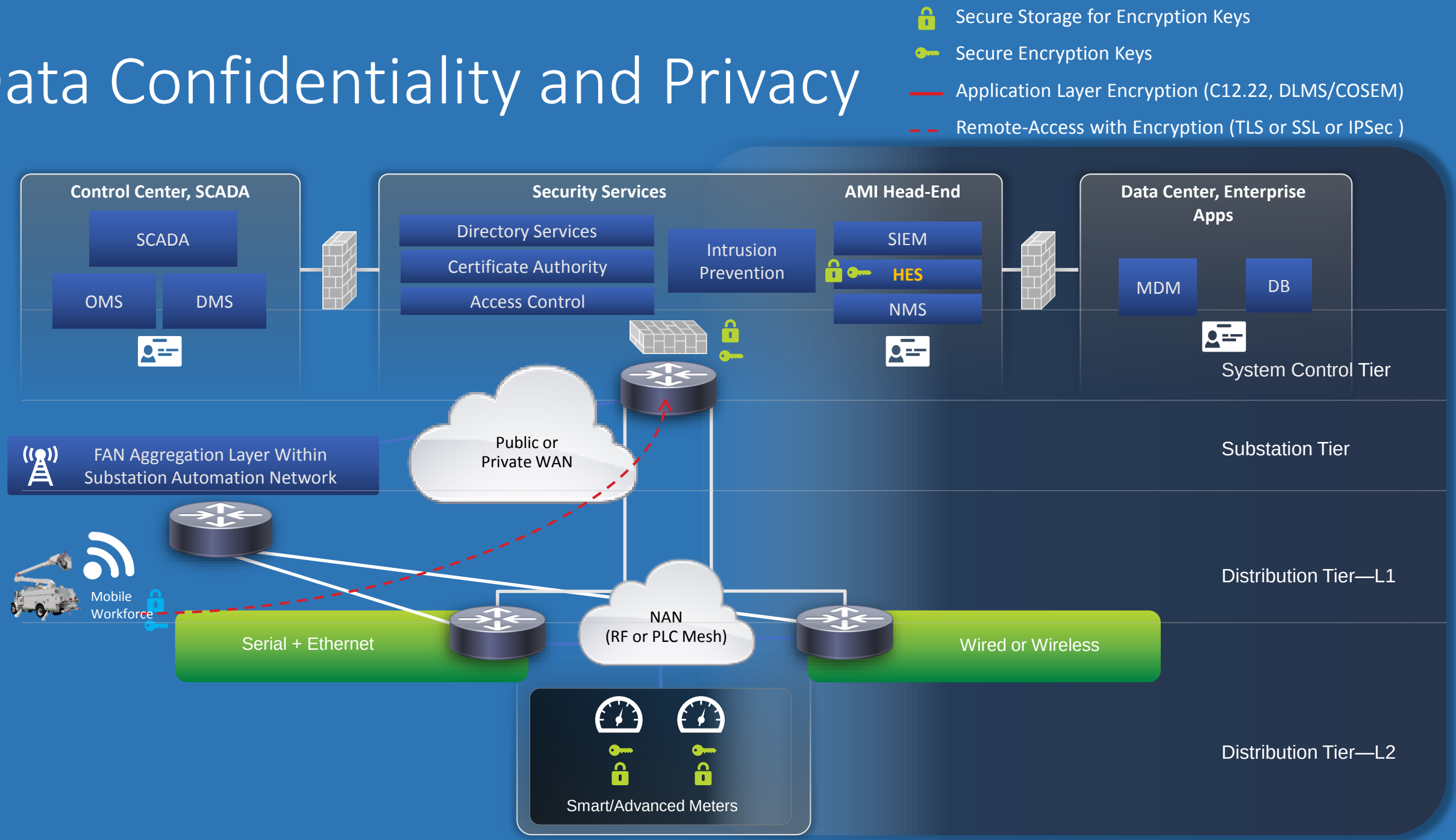
Used in FAN and AMI for:

- Secure generation and storage of encryption keys on all devices—meters, routers, application servers such as AMI Head End, NMS
- Encrypting all data traversing using IPSec over public networks between substations and control center or between substations
- Link-layer (mesh) encryption of data from meters to the field area routers and network layer encryption from FAR to AMI Head End (IPSec)
- (Optional) Application layer encryption of meter readings

Data Confidentiality and Privacy



Data Confidentiality and Privacy



Threat Detection and Mitigation

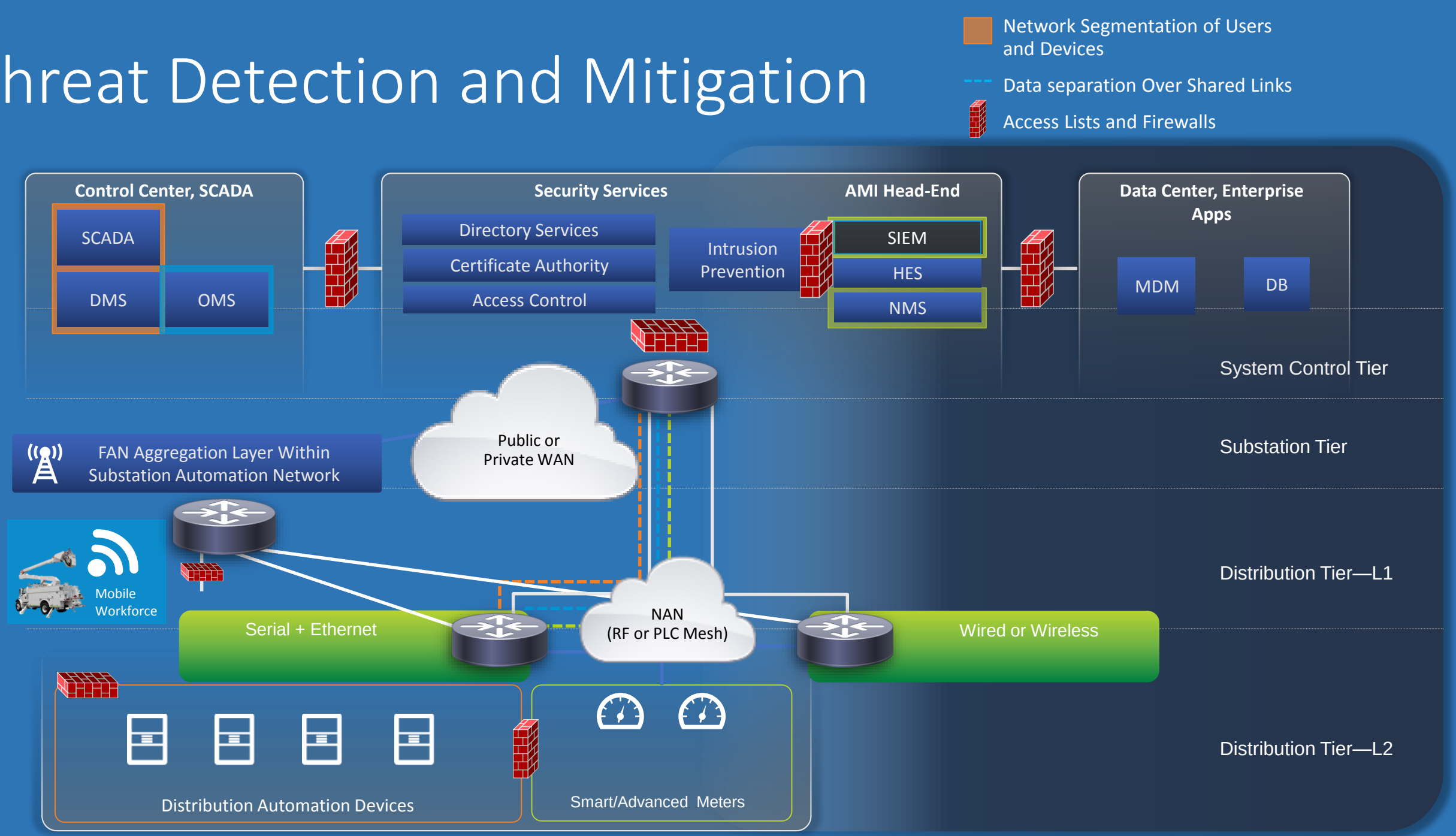
Purpose: Protect critical assets against cyber attacks and insider threats

Components: VRF and VLAN, access lists, Firewall and Intrusion Prevention (on routers and appliances), device logs, SIEM

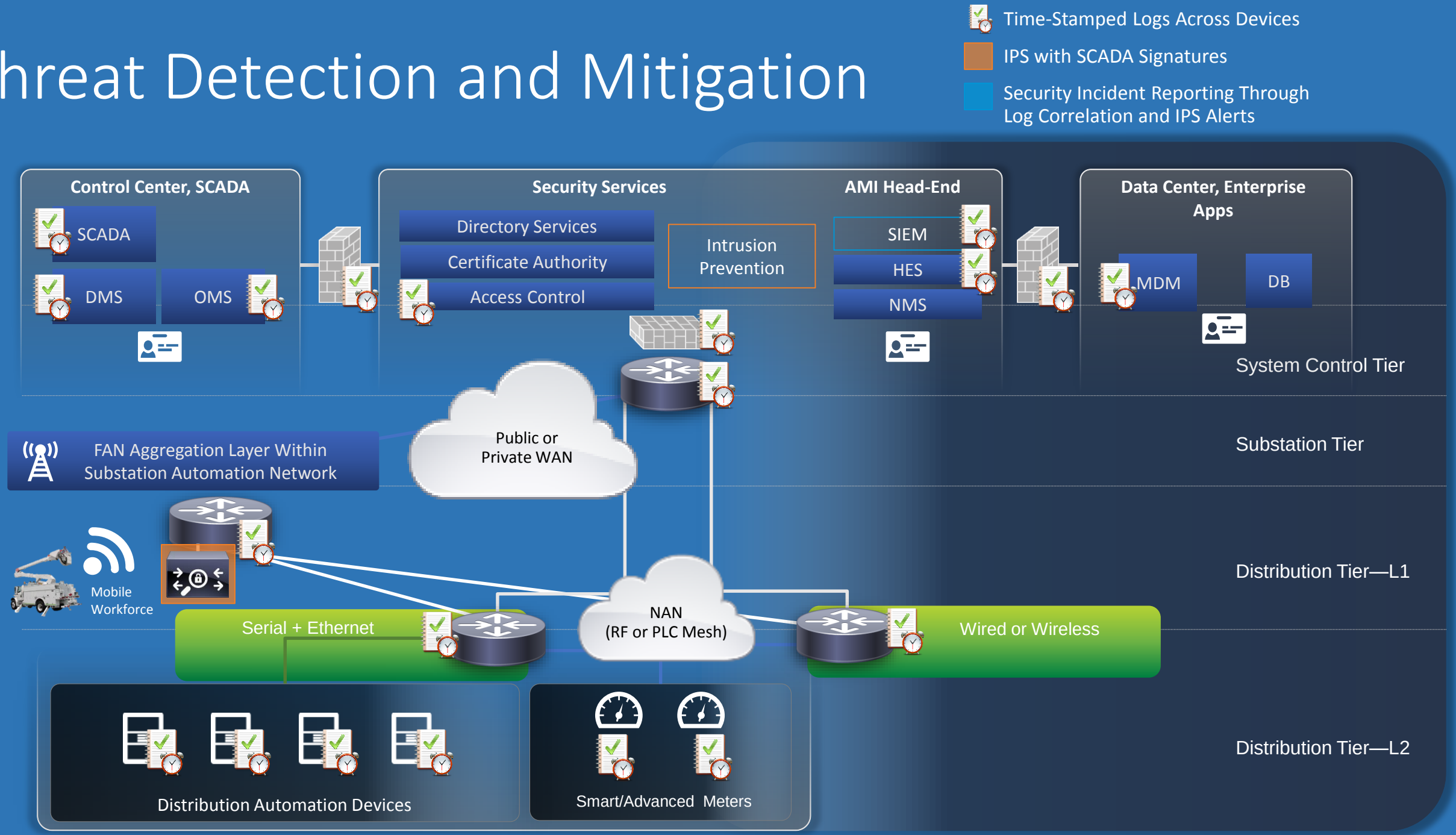
Used in FAN and Substation for:

- Logically segment and separate traffic—AMI vs. DA vs. mobile workforce
- Use access-lists to filter traffic between segments/zones
- Deploy firewalls to protect critical assets and create a layered network based on stricter restrictions with increasing security levels
- Detect network intrusions through use of IPS at critical points in the network. (Optional) customize with SCADA IPS signatures
- Collect logs across devices, meters, application and correlate with IPS events to identify security incidents with SIEM, take mitigation steps

Threat Detection and Mitigation



Threat Detection and Mitigation



Device and Platform Integrity

Purpose: Ensure that devices and meters are cannot be compromised easily and are resistant to cyber attacks

Components: Tamper-resistant design, digitally signed firmware images, NIST-approved or equivalent cryptographic algorithms, secure storage of cryptography credentials, secure code development practices

Used in FAN and Substation for:

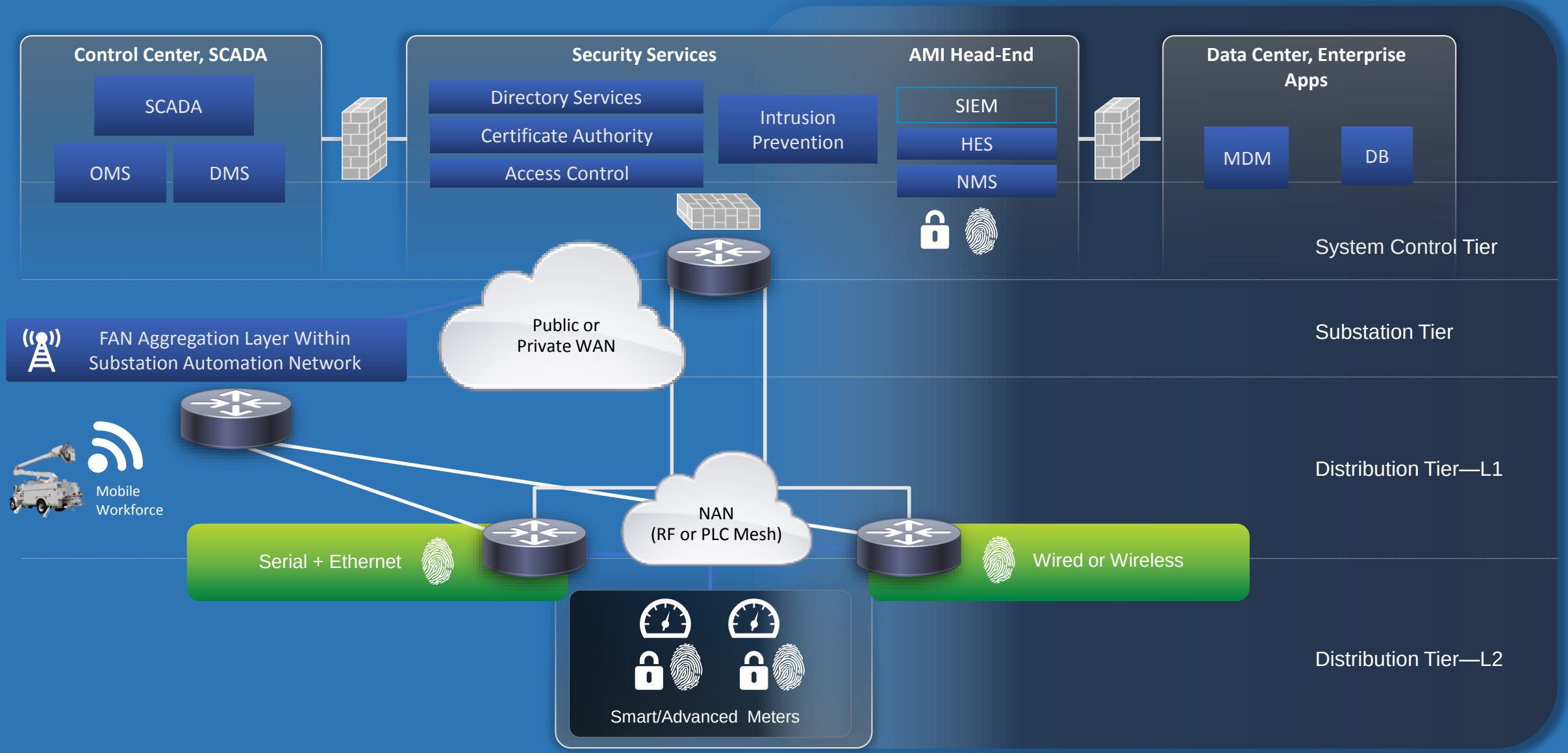
- Tamper-resistant design for meters and devices, trigger alerts on physical tampering, maintain local audit trail for all sensitive events
- Validate the authenticity and integrity of firmware upgraded on meters, routers and devices and software patches on grid applications
- Ensure the critical commands are not altered or corrupted
- Use of rate-limiting and other throttling mechanisms against DoS attacks
- Secure code development lifecycle including strong practices around publishing security vulnerabilities, releasing workarounds

Device and Platform Integrity

Digitally Signed Commands From Head-End System (HES) to Meters

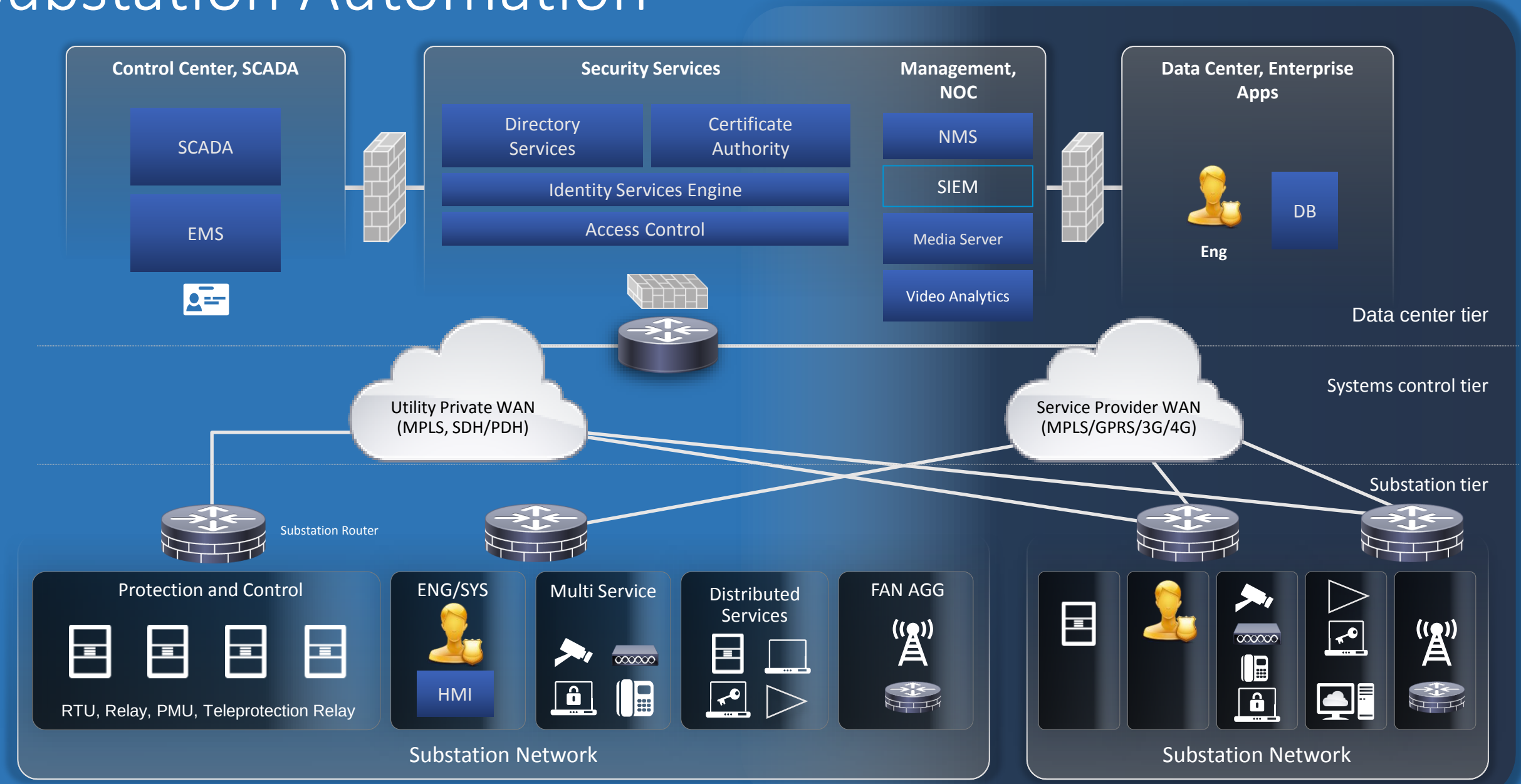
Authenticated Data From Meter Registers

Digitally Signed Firmware Images



Substation Networks

Substation Automation



Access Control

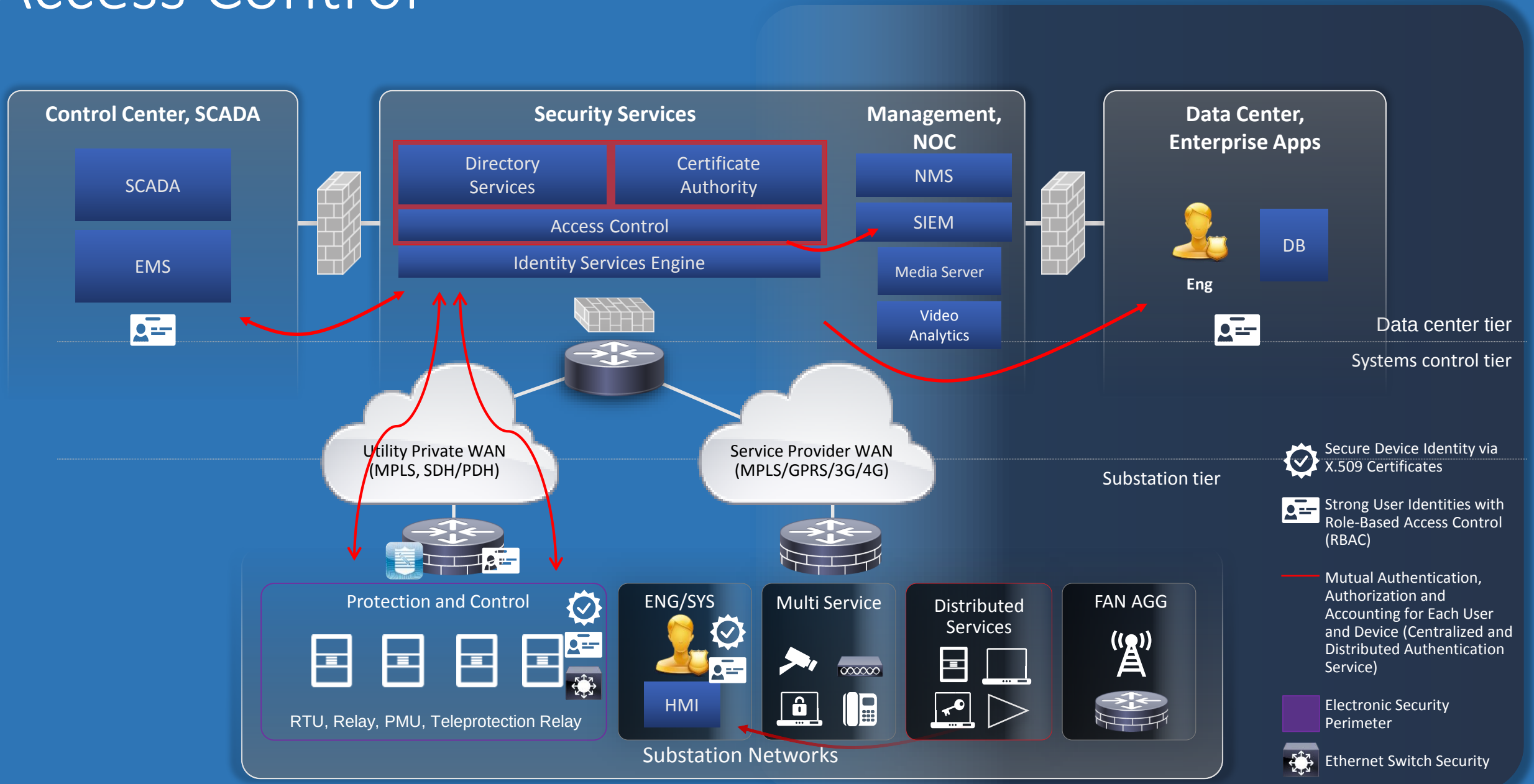
Purpose: Ensure that only authorized personnel are accessing the network and valid devices are part of the grid network

Components: Role-Based Access Control with i) username and passwords ii) X.509 certificate based identities; RADIUS and TACACS+ protocols for Authentication, Authorization and Accounting (AAA) for users and devices; Network Admission Control (NAC), Infrastructure Security

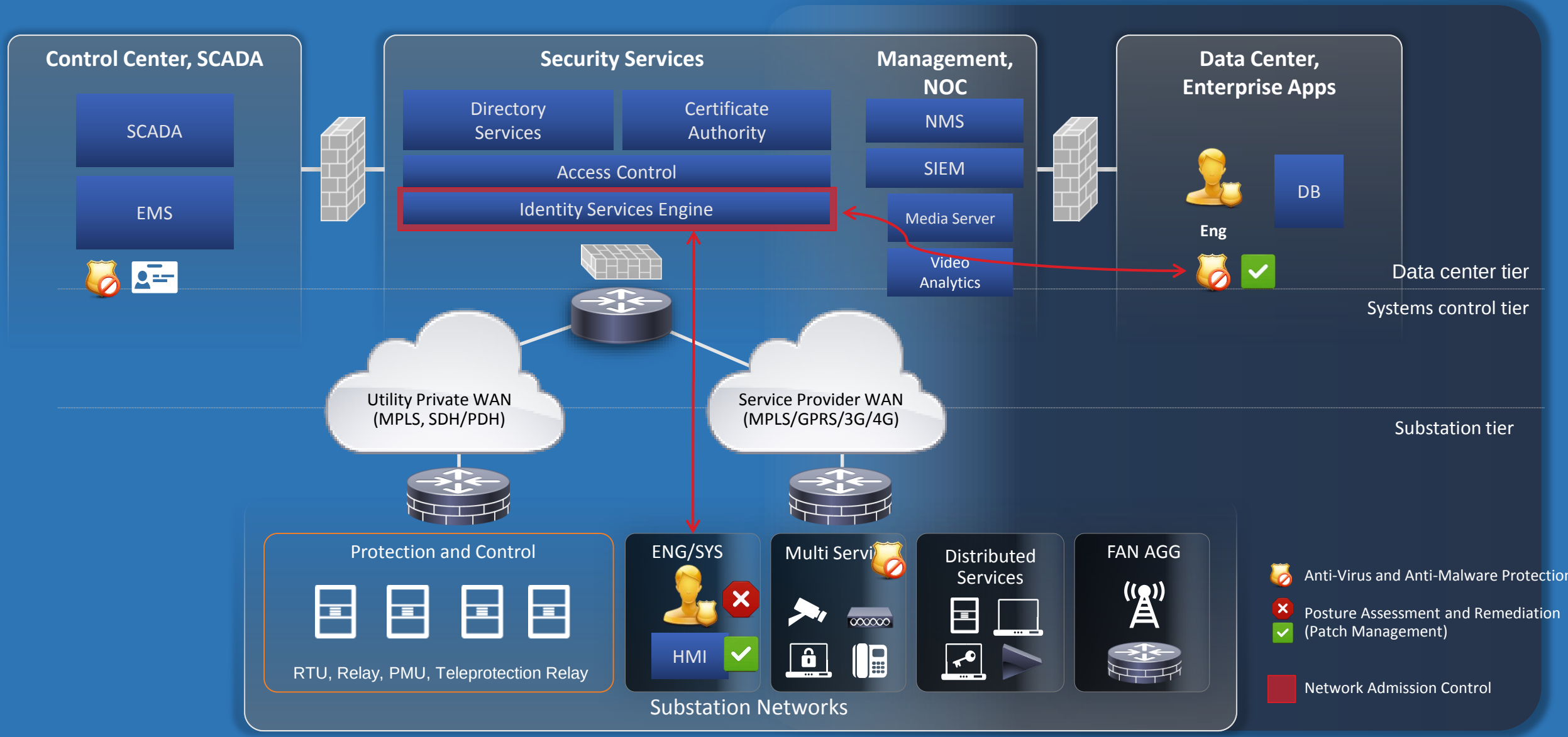
Used in Substation and Control Center for:

- Authenticating and authorizing field technicians or operations center staff before they can view or configure devices, track changes made (RBAC)
- Authentication and RBAC through IEC 62351 extensions for TC57 protocol suite
- Authenticating every device and application connected to the substation and control center networks—routers, switches, servers, workstations, IEDs, reclosers, RTU's, Relays etc
- Mutually authenticating user and supported devices by relying on strong certificate based identities
- End point posture assessment of for devices as laptops, workstations, servers connecting to Substation/CC LAN segments to detect any viruses or worms before allowing access to the network, forcing remediation such as installing software patches or updating anti-virus database

Access Control



Access Control



Data Confidentiality and Privacy

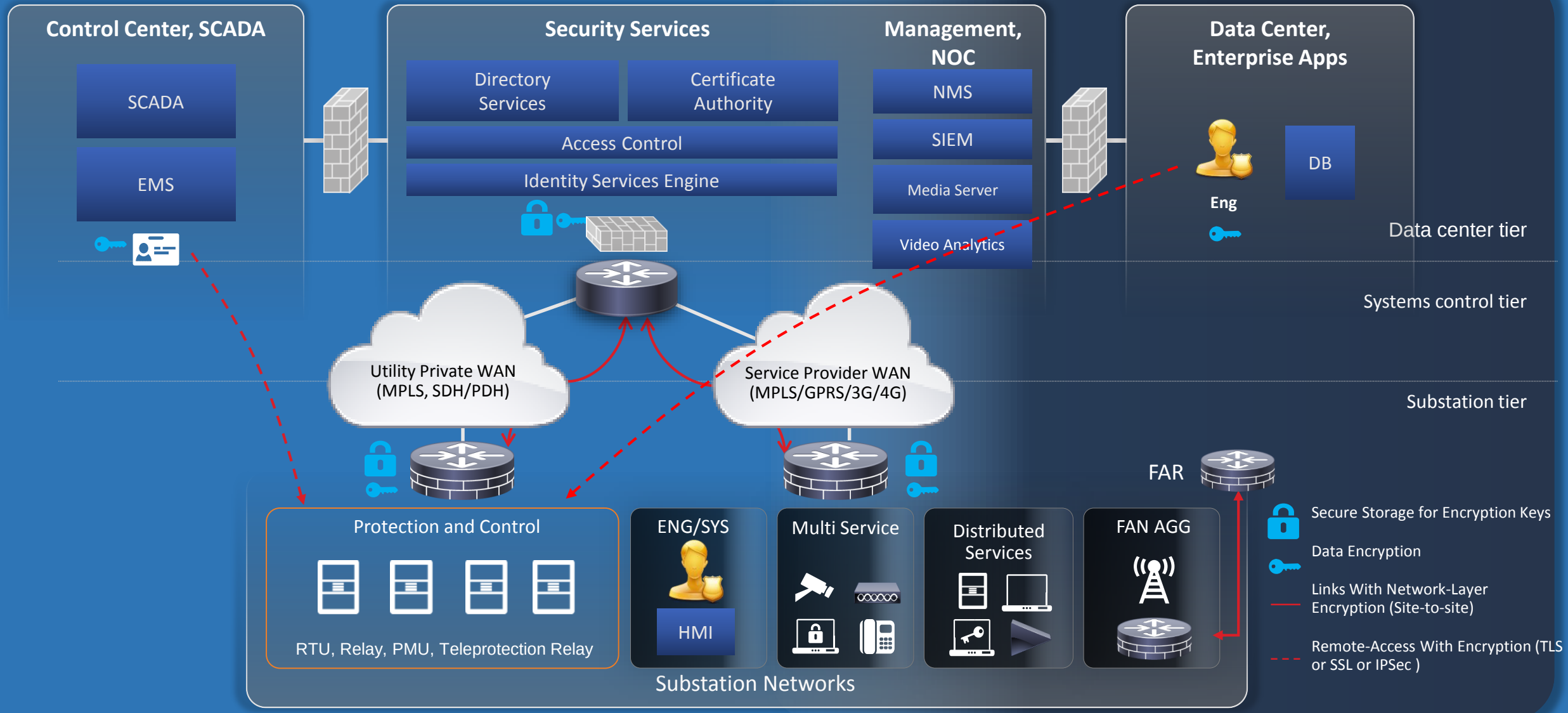
Purpose: Ensure data privacy and data integrity for operational and control data used in utility operations

Components: X.509 Certificate, IPSec with flexible VPN architectures, link-layer and application layer encryption mechanisms, Scalable crypto key management like DMVPN or GETVPN over both Service Provider or privately owned utility networks.

Used in Substation and Control Center for:

- Secure generation and storage of encryption keys on all devices, routers, IPSec Head Ends and provisioning systems as NMS
- Encrypting all data traversing using IPSec over public or private networks between substations and control center or between substations as necessary
- (Optional) Authentication and encryption through IEC 62351 extensions for TC57 protocol suite

Data Confidentiality and Privacy



Threat Detection and Mitigation

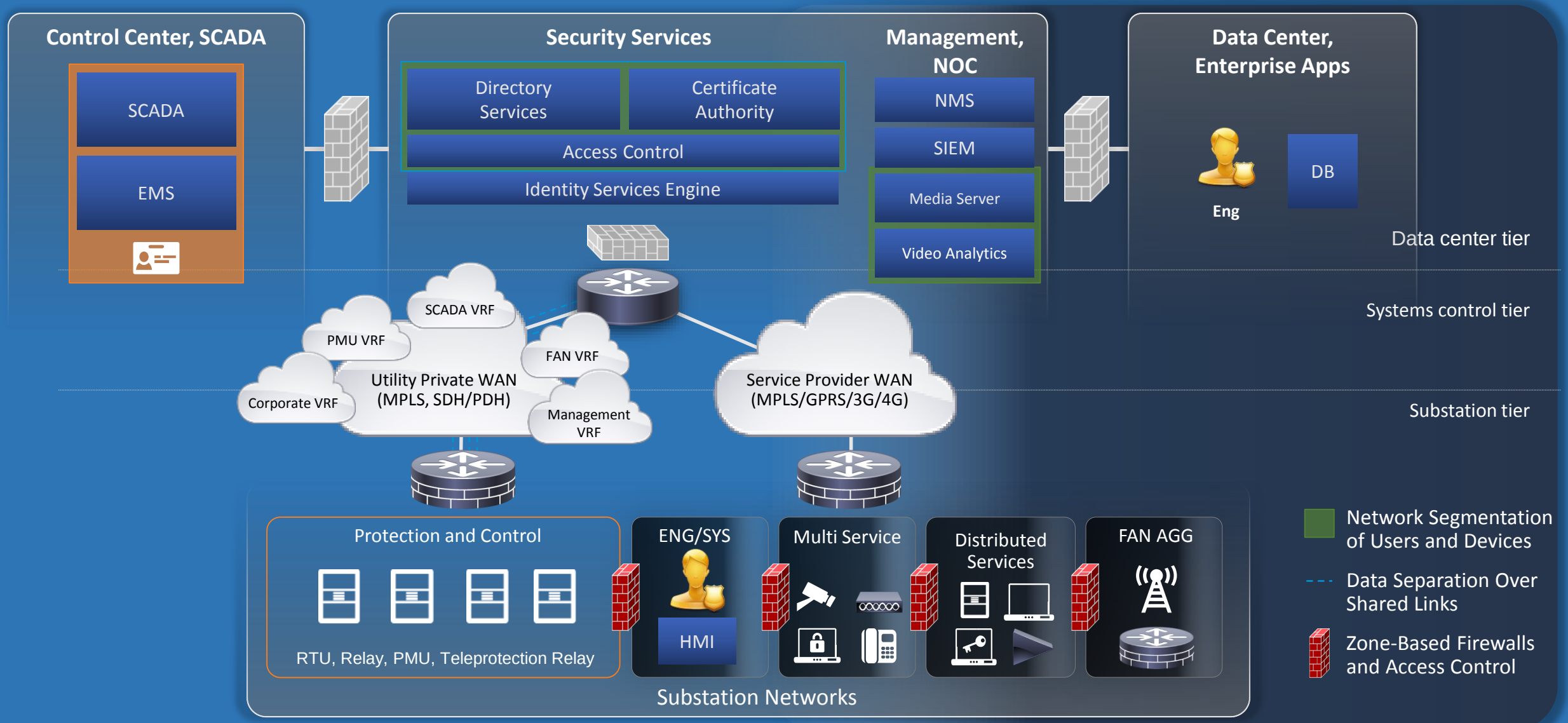
Purpose: Protect critical assets against cyber attacks and insider threats

Components Segmentation (VRF, MPLS VPN and VLAN), access lists, Firewall and Intrusion Prevention (on routers and appliances), Syslog, NetFlow, SIEM, IP SLA's

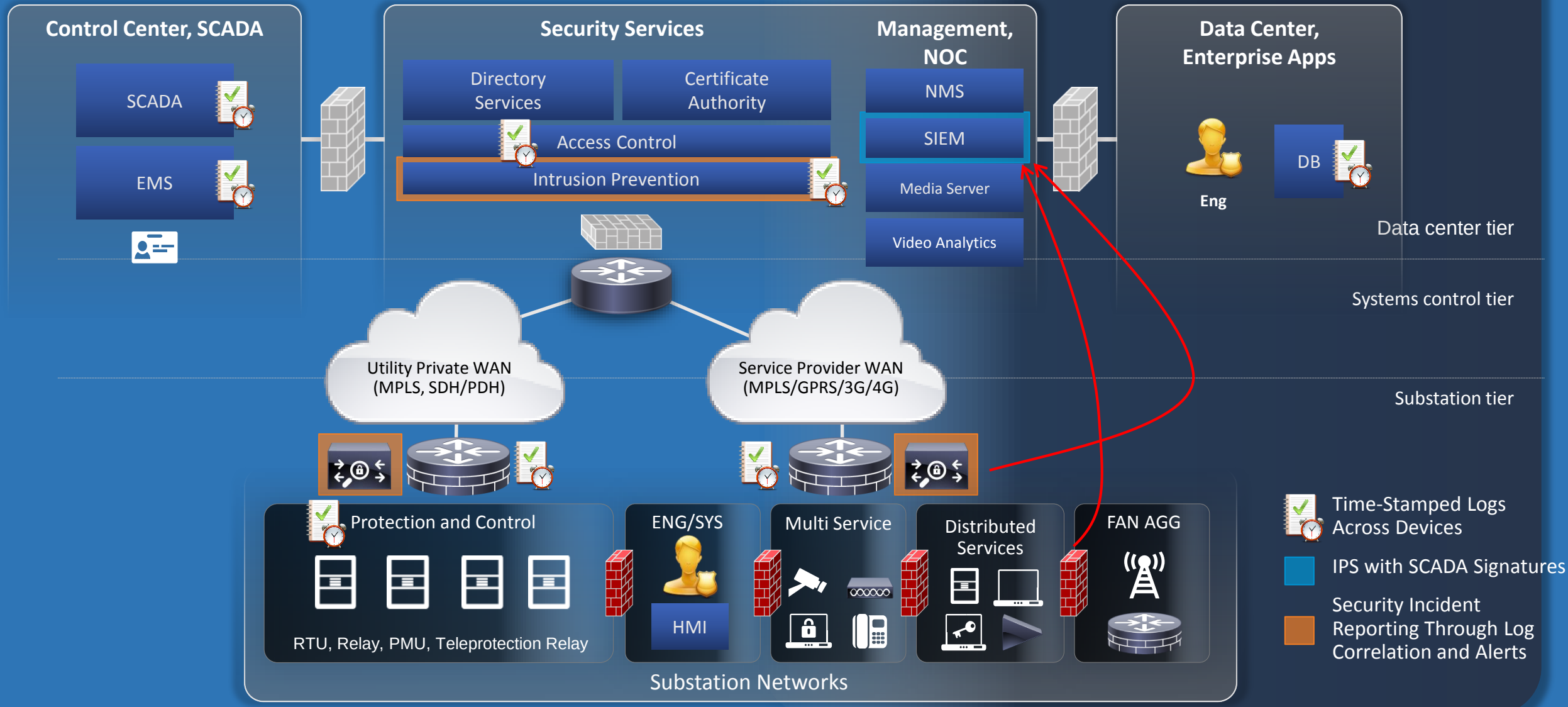
Used in FAN and SA for:

- Logically segment and separate traffic based on application class e.g. SCADA, Engineering, PMU, Physical Security
- Access-lists to filter, log and authorize traffic between segments/zones.
- Define and protect ESP Access point boundary as per NERC/CIP requirements to protect critical assets and create a multilayer security functions.
- Detect network intrusions through use of IPS/IDS at critical points in the network. (Optional) customize with SCADA IPS signatures
- Collect logs across devices, meters, application and correlate with IPS events to identify security incidents with SIEM, take mitigation steps

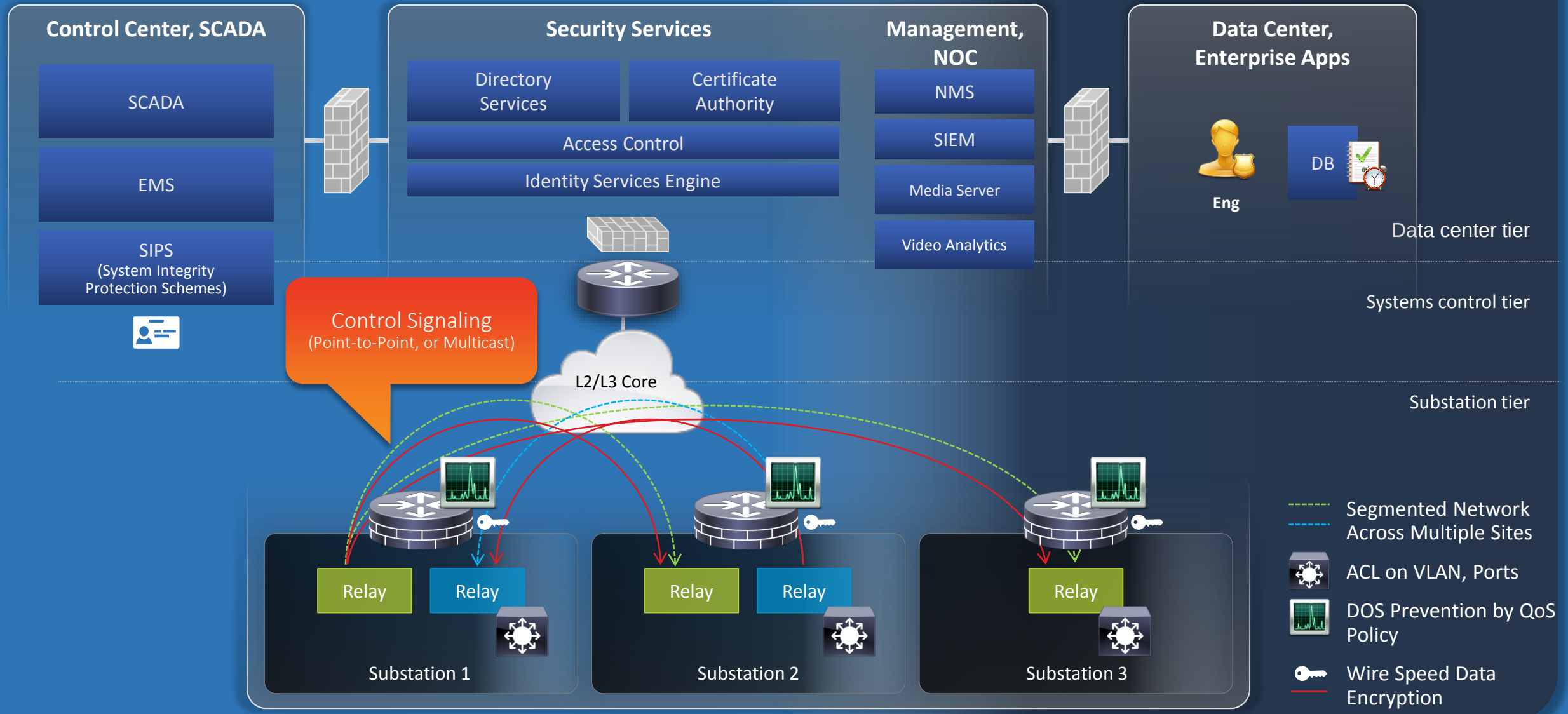
Threat Detection and Mitigation



Threat Detection and Mitigation

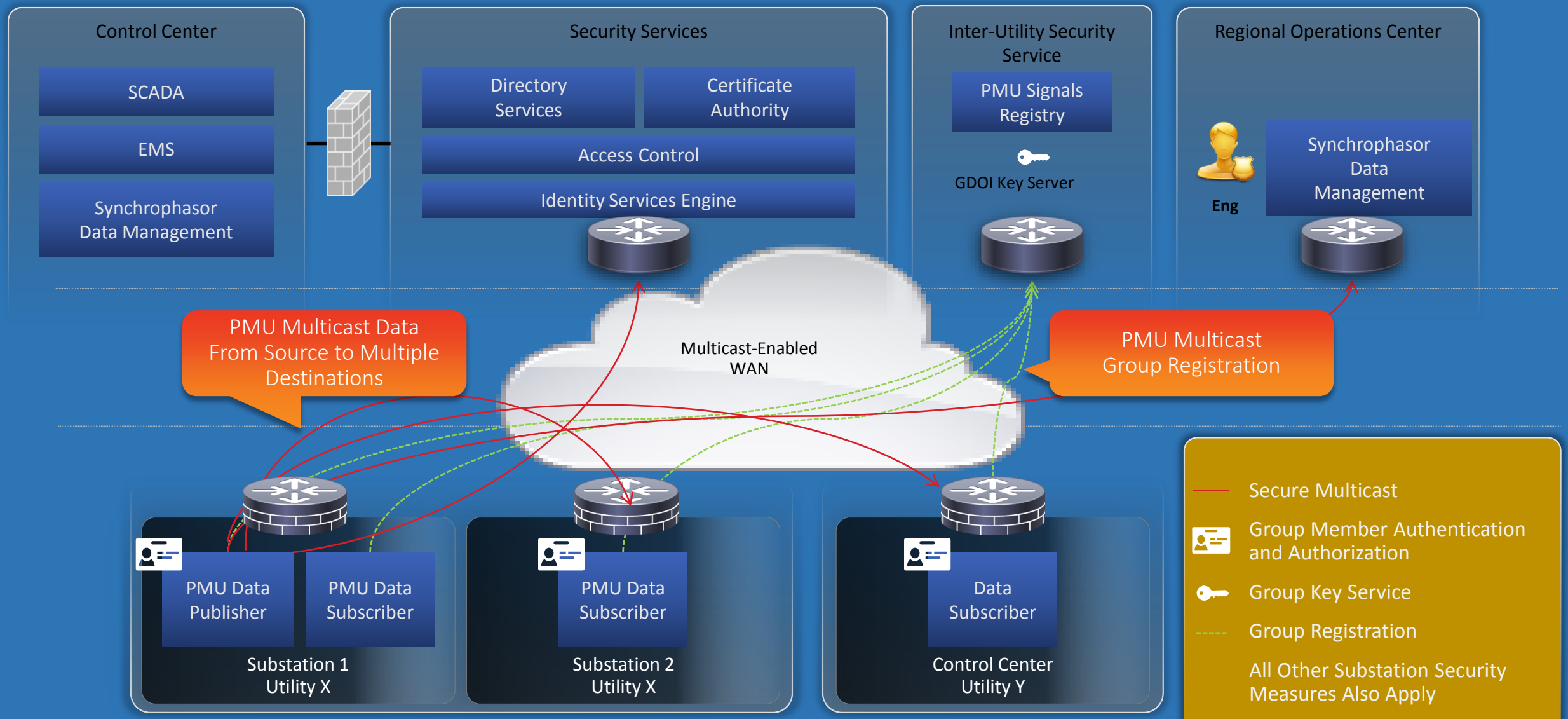


Threat Detection and Mitigation



PMU & Wide Area Networks

PMU Network

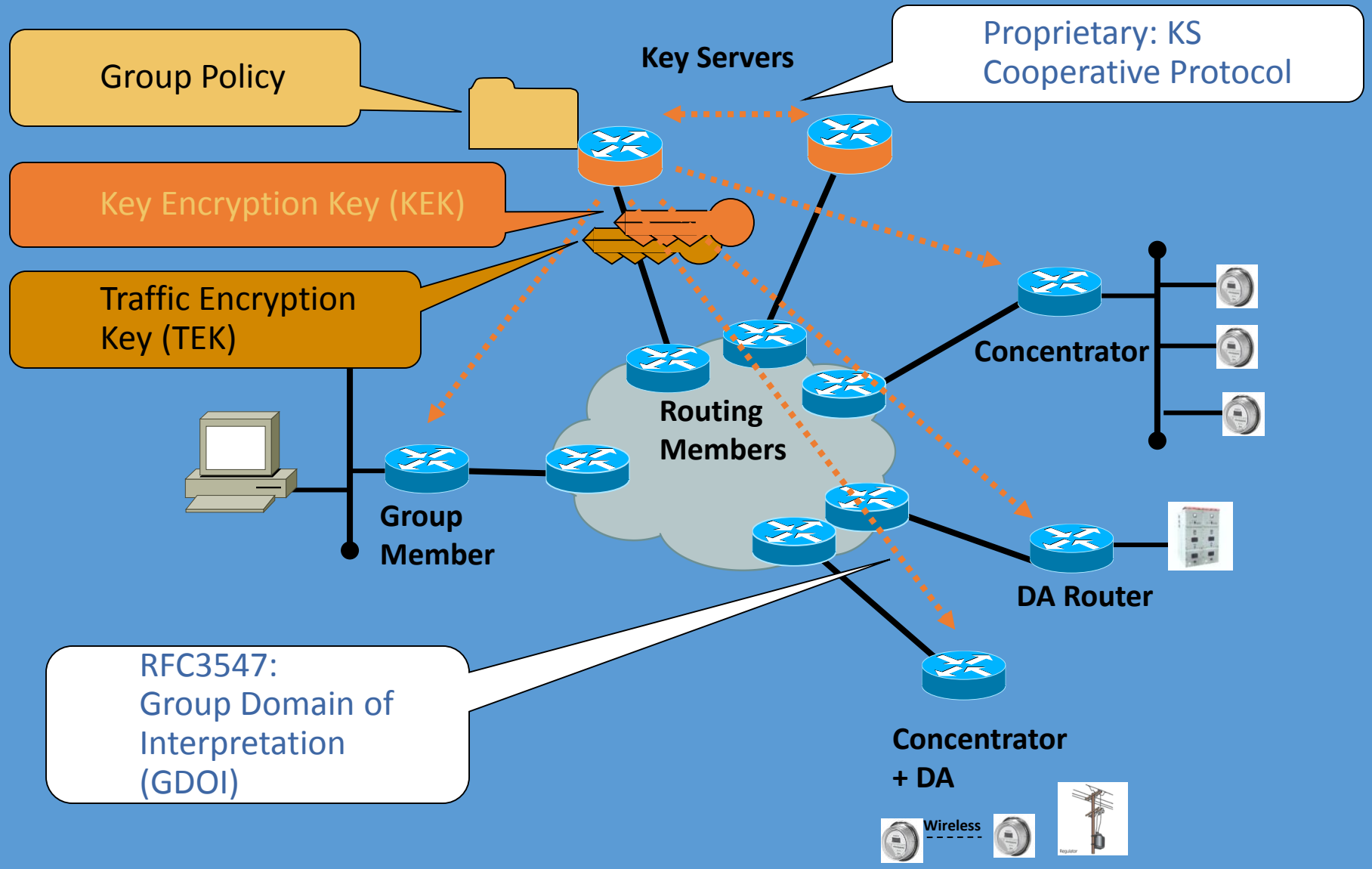

Control Center
SCADA
EMS
Synchrophasor Data Management
Security Services
Directory Services
Certificate Authority
Access Control
Identity Services Engine
Inter-Utility Security Service
PMU Signals Registry
GDOI Key Server
Regional Operations Center
Eng
Synchrophasor Data Management
PMU Multicast Data From Source to Multiple Destinations
Multicast-Enabled WAN
PMU Multicast Group Registration
PMU Data Publisher
PMU Data Subscriber
Substation 1 Utility X
PMU Data Subscriber
Substation 2 Utility X
Data Subscriber
Control Center Utility Y
Secure Multicast
Group Member Authentication and Authorization
Group Key Service
Group Registration
All Other Substation Security Measures Also Apply

Group Crypto for WANs

Group Encryption in the Wide Area Network

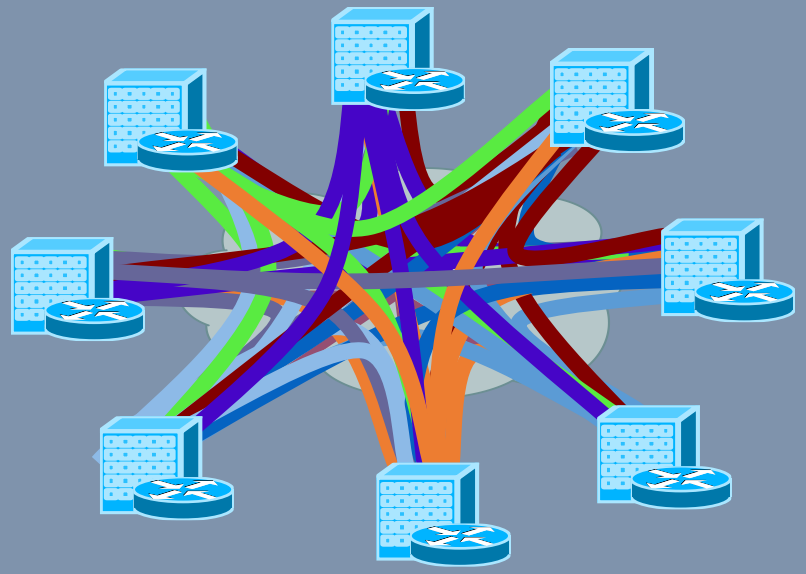
- Group Encrypted Transport VPN
- Leverage one Security Association per Virtual Network (per VNET/VRF)
- Allows for any to any conversation
- Distributes the Key server function
  - no single point of failure
- GETVPN has a robust approach for Key Server load balancing and reliability

Group Security Elements



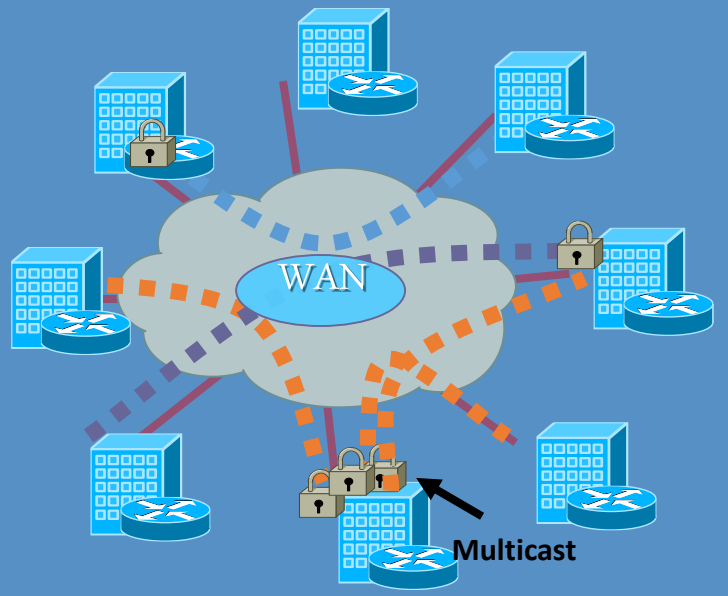
Any-to-Any Encryption

IPsec Point-to-Point Tunnels



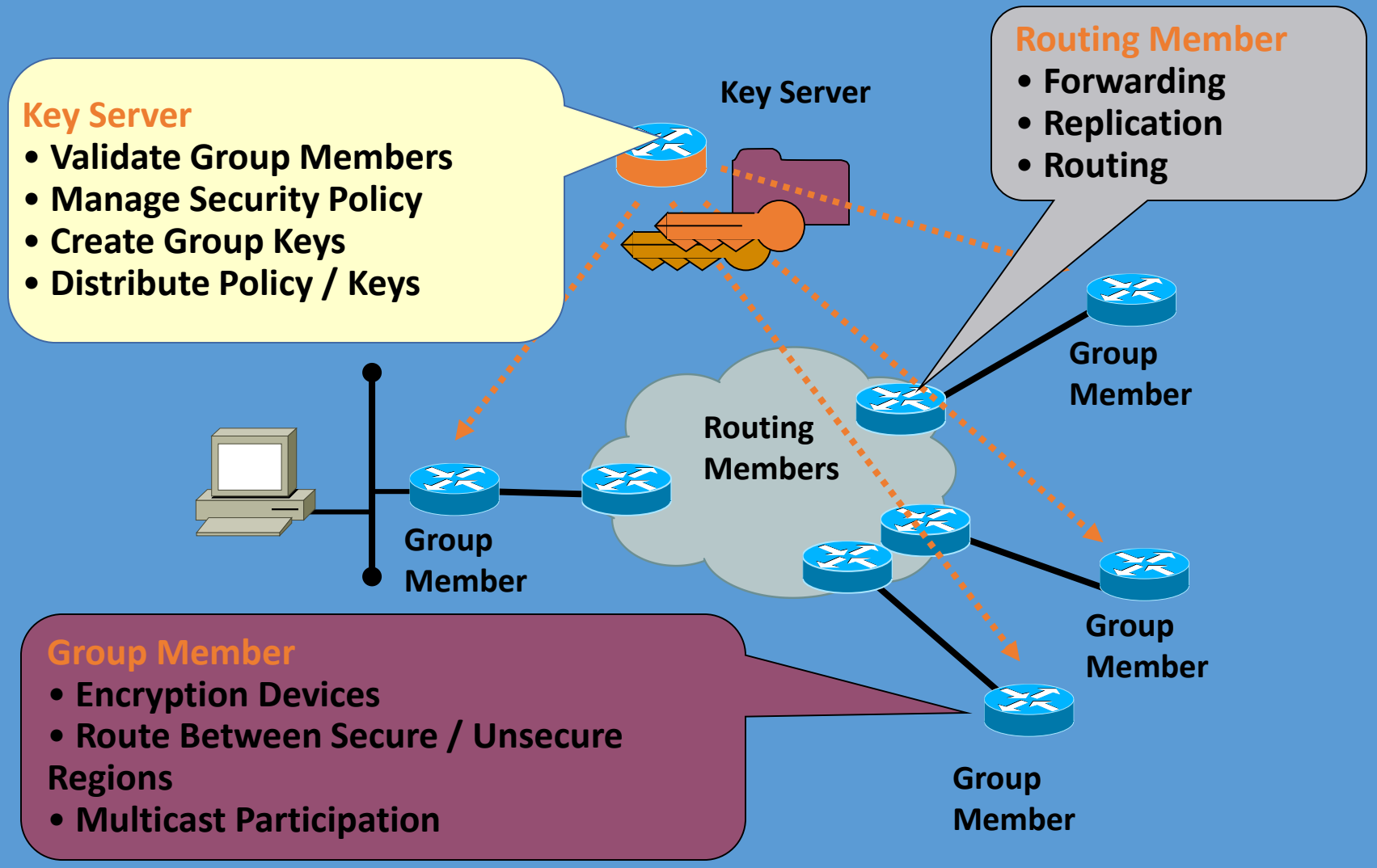
- Scalability—an issue (N^2 problem)
- Any-to-any instant connectivity can't be done to scale
- Overlay routing
- Limited advanced QoS
- Multicast replication inefficient

Tunnel-less Group VPN



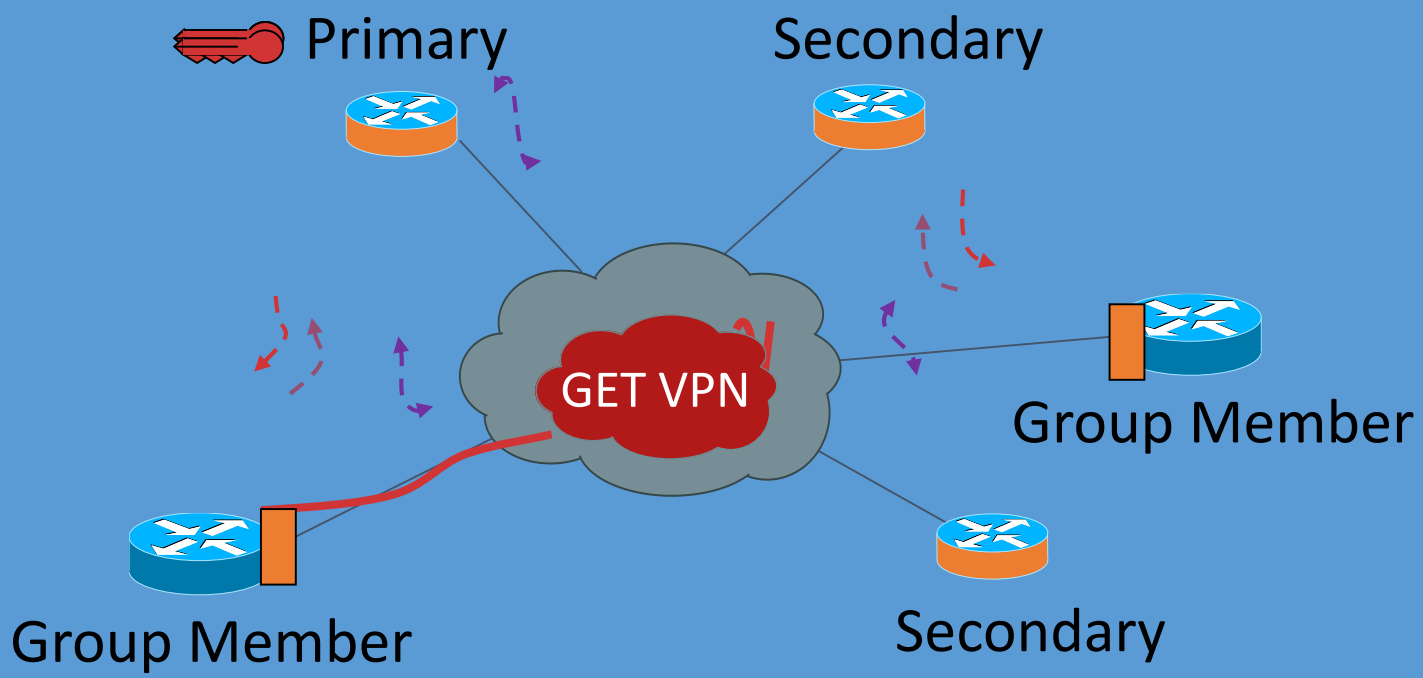
- Scalable architecture
- Any-to-any instant connectivity to high-scale
- No overlays – native routing
- Advanced QoS
- Efficient Multicast replication

Group Security Functions

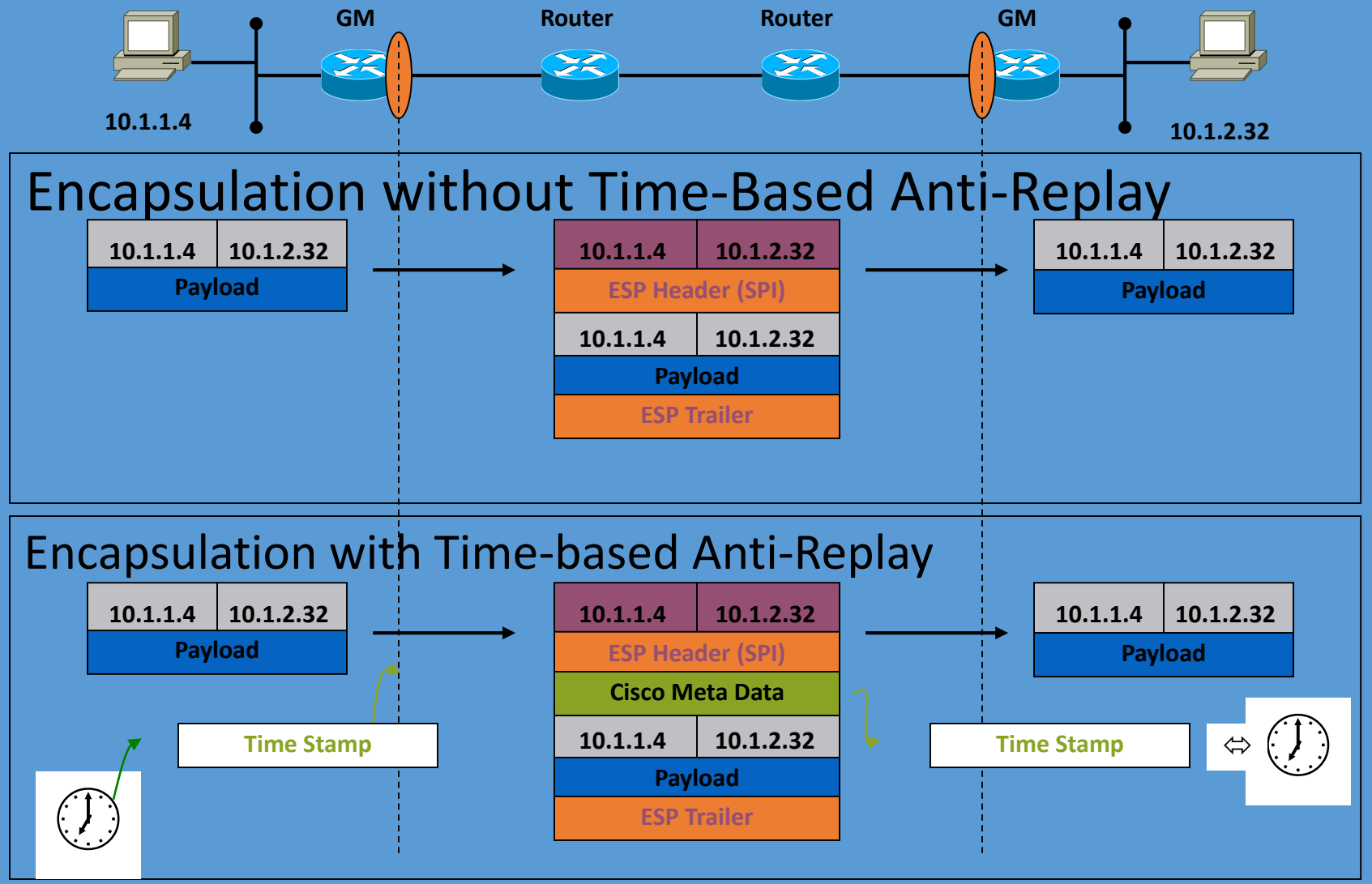


Cooperative Key Server: Roles

- Primary: Elected by eligible set of KS
  - Creates Keys, Registers GM, Distributes Keys, Notifies Secondary
- Secondary: Eligible KS in cooperative state for a group
  - Registers GM, Monitors Primary, Notifies Primary of New GM

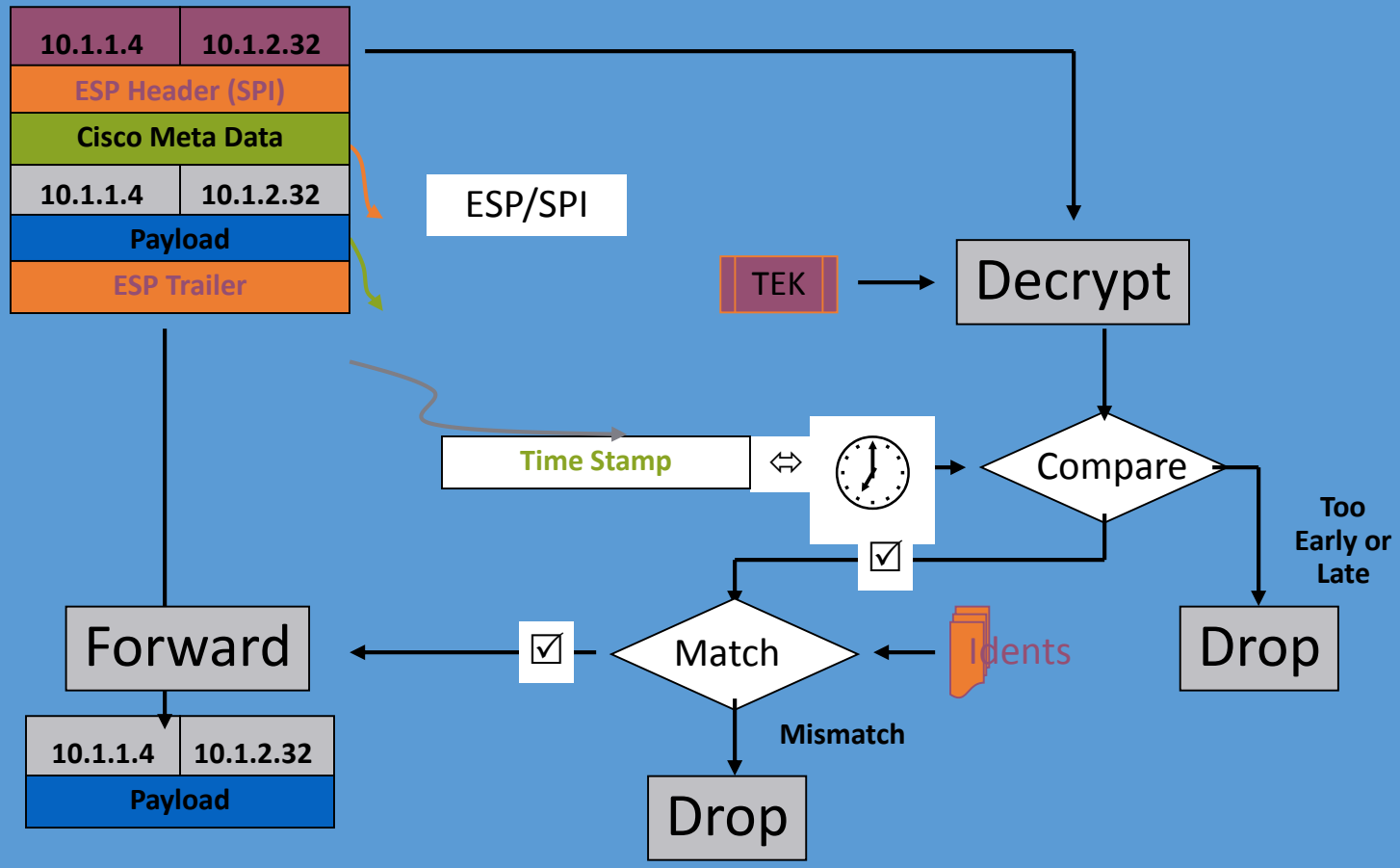


Group Encrypted Transport (Data Plane Encapsulation)



Group Encrypted Transport (Data Plane Processing)

- Group Member Receive Processing

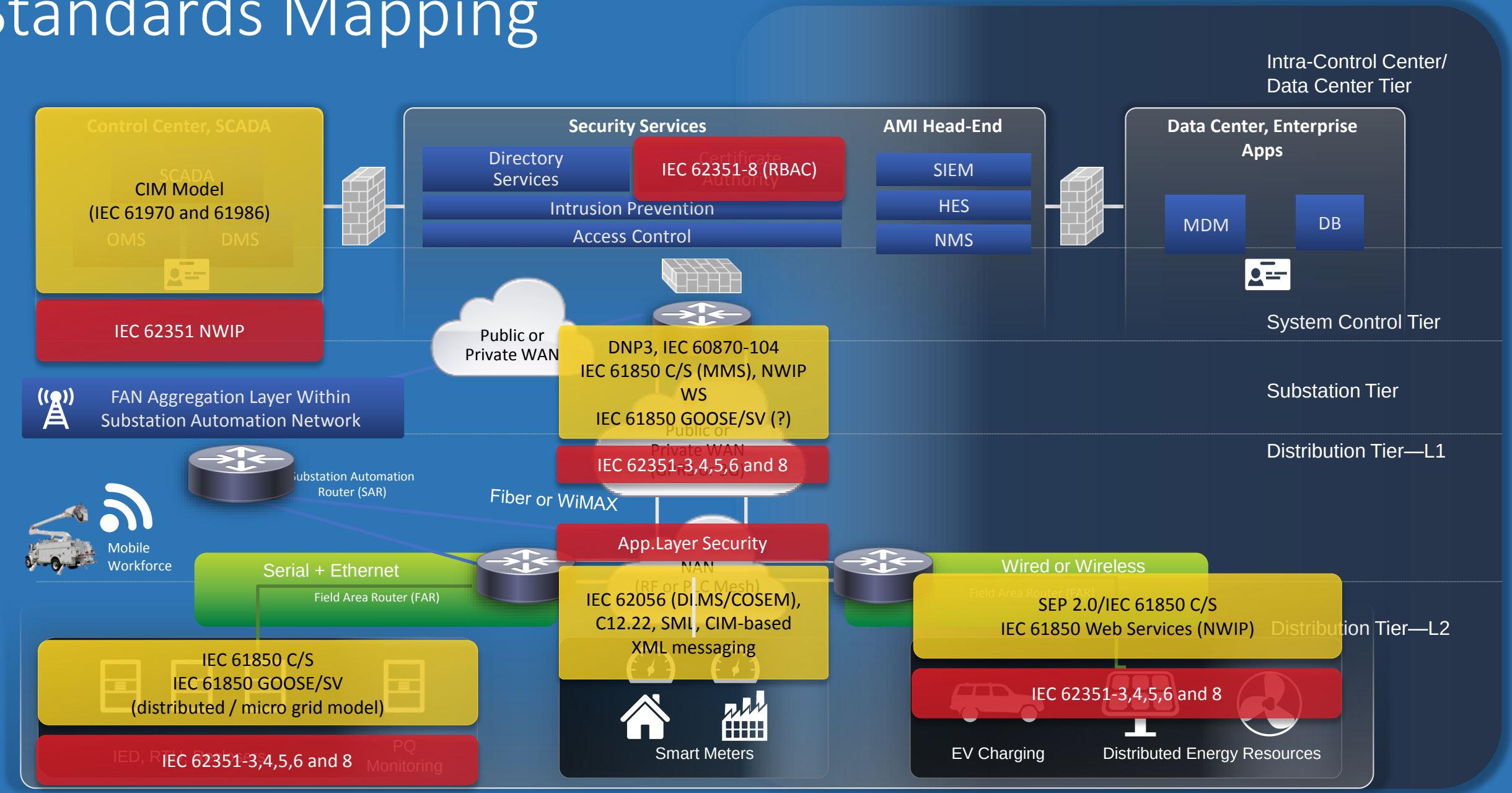


IEC Standards for Security

Standard Descriptions (IEC 62351)

- Part 1/2: Introduction and Domain specifics/Glossary
- Part 3: Security for protocols based on TCP/IP (ICCP/TASE.2, 61850 C/S)
- Part 4: Security for protocols based on MMS (ICCP/TASE.2, 61850 C/S)
- Part 5: Security for IEC 60870-5 and Derivatives (IEC 60870-5-104 and DNP3, IEC 60870-5-101,102,103 and Serial DNP)
- Part 6: Security for IEC 61850 (MMS, GOOSE, SV)
- Part 7: Network and system management (NSM) data object models
- Part 8: RBAC for power system management
- Part 9: Key Management (Approved NWIP)
- Part 10: Security for CIM and data at rest (NWIP)

Standards Mapping



Standards Mapping