MPLS JAPAN

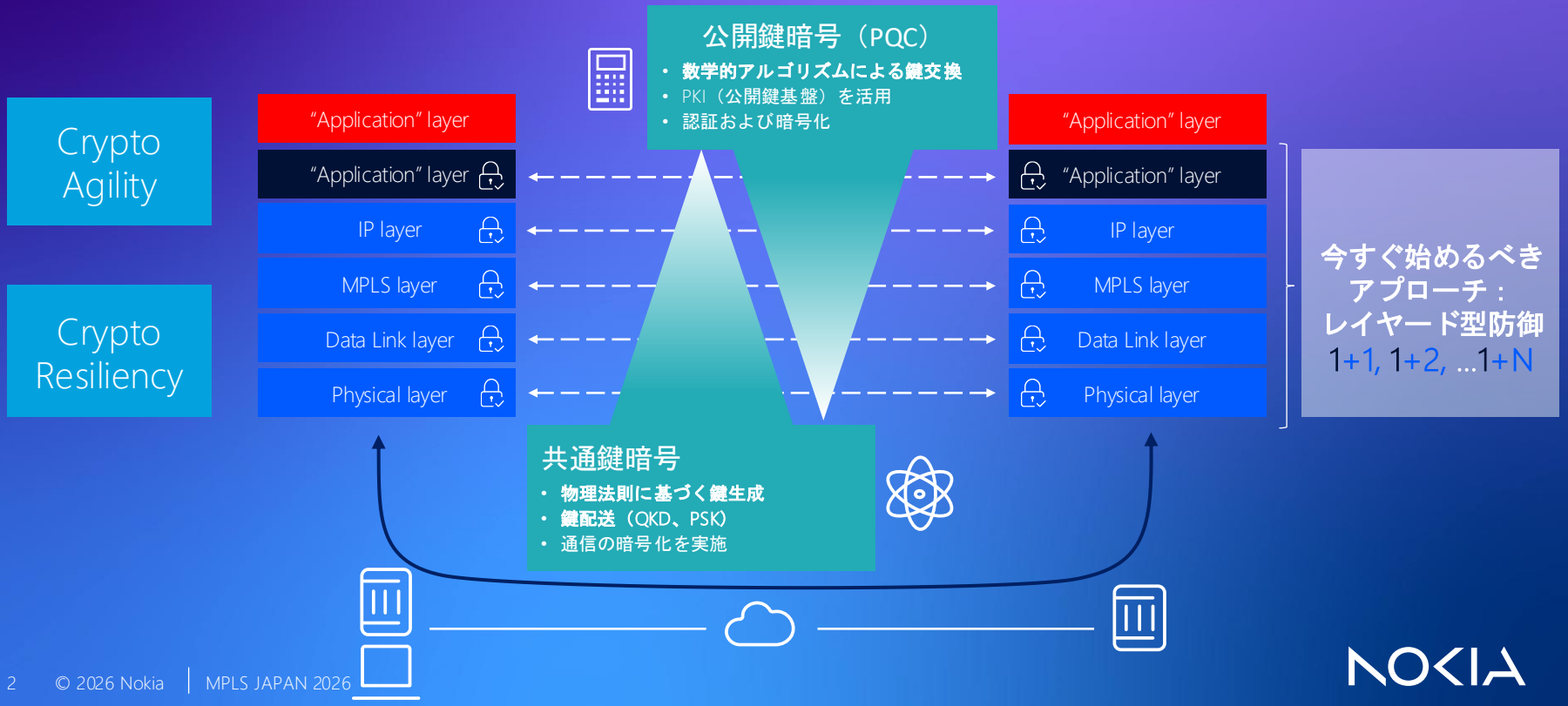
MACsec標準の拡張によるQSNの実現とPSKベースの実装例

鹿志村康生
yasuo.Kashimura@nokia.com

© 2026 Nokia

量子安全ネットワークのための多層防御アプローチ

公開鍵暗号と共通鍵暗号を組み合わせた多層防御



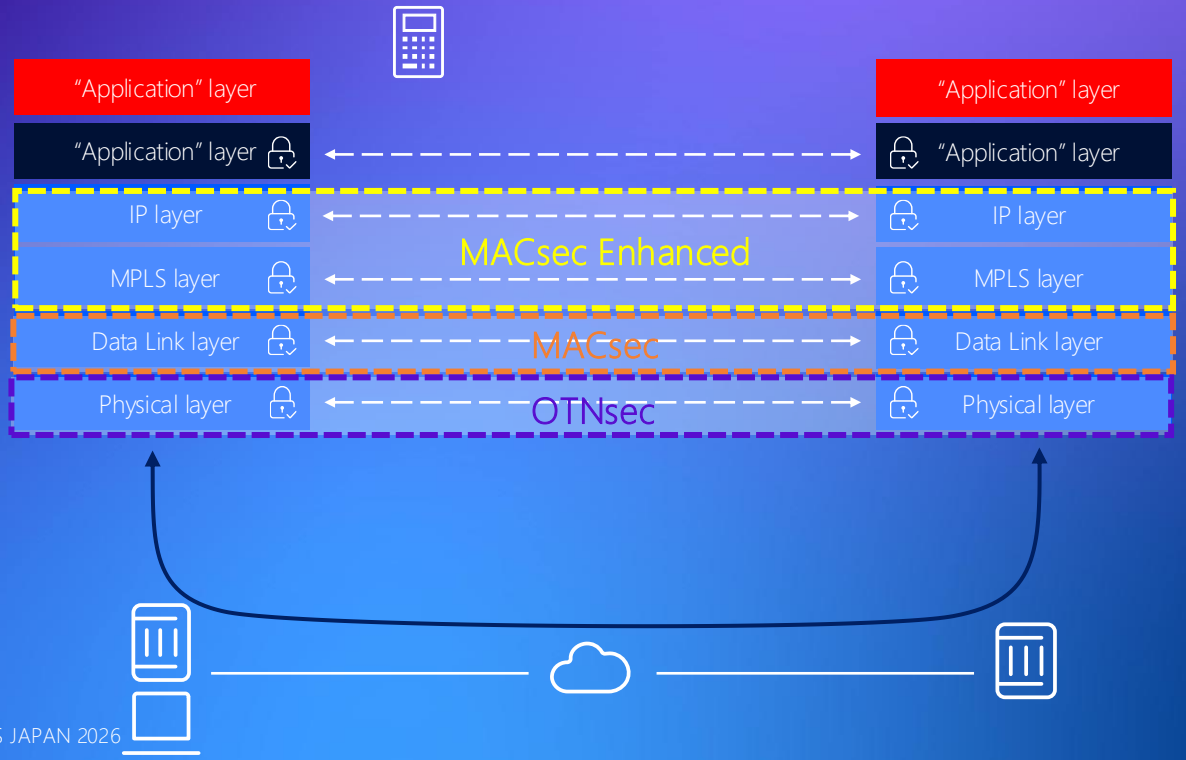
© 2026 Nokia

量子安全ネットワークのための多層防御アプローチ

公開鍵暗号と共通鍵暗号を組み合わせた多層防御

Crypto Agility

Crypto Resiliency

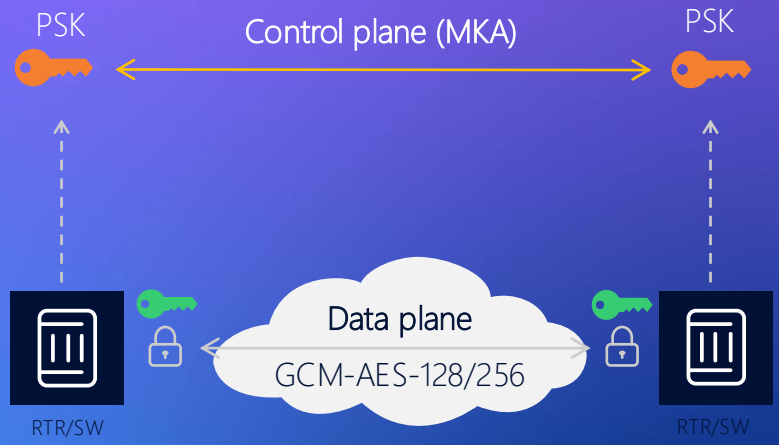


今すぐ始めるべきアプローチ：
レイヤード型防御
1+1, 1+2, …1+N

© 2026 Nokia

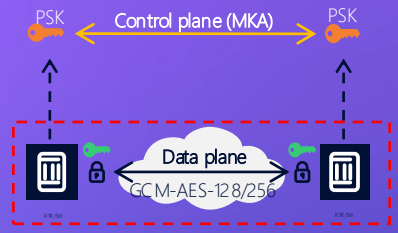
MACsec概要(1)
Ethernetレイヤでの暗号化

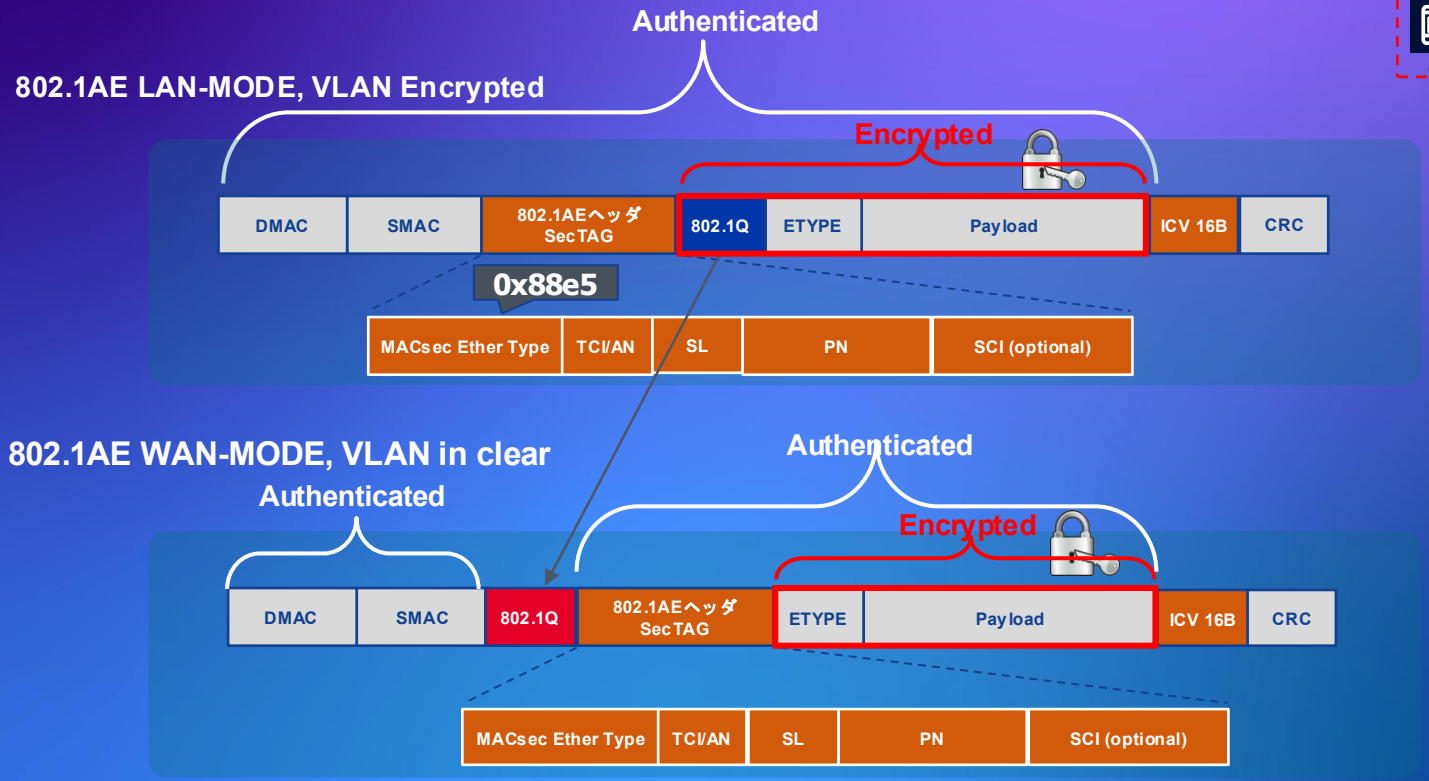
- IEEE 802.1AEで規定
- MACレイヤーでのEncryption
- IPsecよりもシンプルなセットアップ
- MKA(MACsec Key Agreement)による鍵交換/管理
- AES128/256でのデータプレーン暗号化
- 比較的安価なSwitch含む多くのEthernet機器(Router/Switch)でHWサポート
  - BCM MACsec PHY, Jericho2c+/3
  - Nokia FP5 chipset(E5)
  - Cisco Silicon One



© 2026 Nokia

MACsec概要(2)
データプレーンフレームフォーマット





TCI: TAG Control Information

AN: Association Number

SL: Short Length

PN: Packet Number

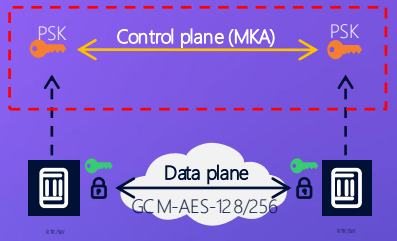
SCI: Secure Channel Identifier

ICV: Integrity Check Value

© 2026 Nokia

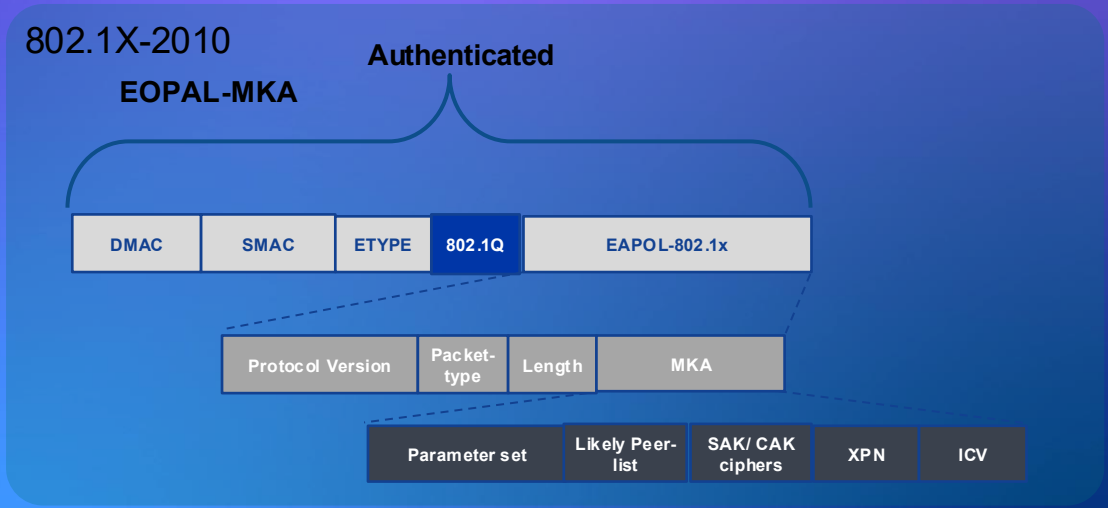
MACsec概要(3)

MKA(MACsec Key Agreement)/コントロールプレーン



MKA (MACsec Key Agreement)

- 802.1xフレームワークを使用、データプレーン暗号化で使用するSKA(Secure Association Key)を交換/管理
- DMACは01:80:c2:00:00:03のMulticast MACをDestinationとする(LLDPと同じ)
- CAK(Connectivity Association Key)を共有しSAKを生成
- MACsecのセキュアチャネルが確率しないとL2プロトコルは動作しない
- 対抗のMACsecデバイス(ピア)を識別しCA(Connectivity Association)を形成
- PNによるリプレイ攻撃防御
- ICV (integrity check value)での整合性検証



© 2026 Nokia

MACsec概要(4)

MACsecでのネットワーク構成

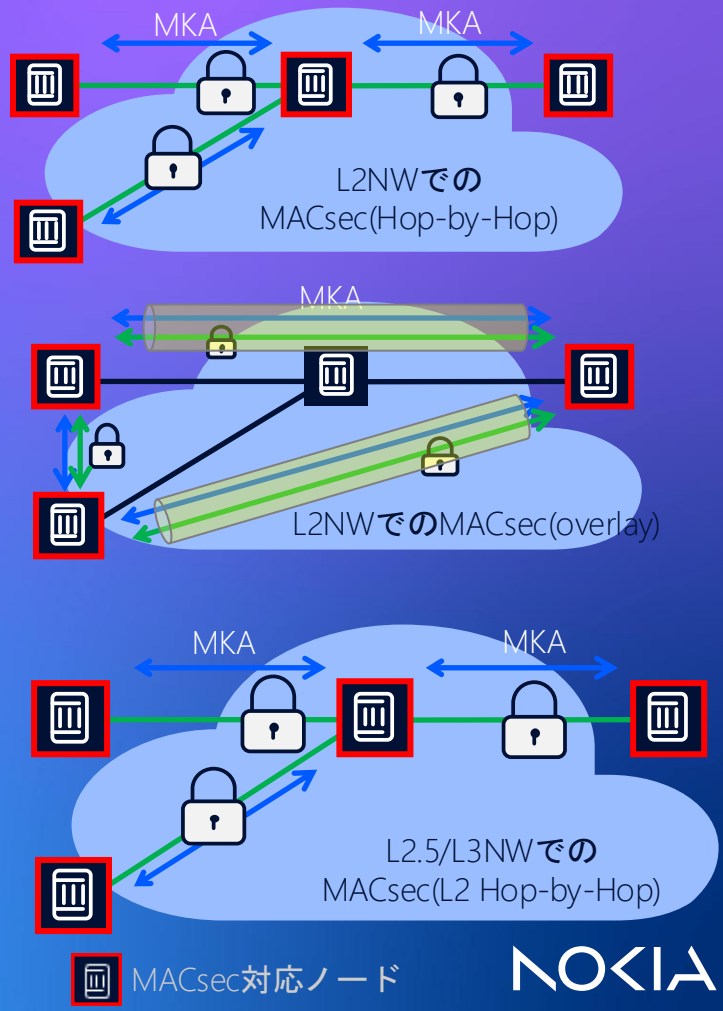
L2ネットワーク(pure-Eth/over L2svc)

- 802.1xパケットのtunneling、WAN-modeの使用等でoverlay L2でのEnd-to-End L2暗号化が可能
- Per-port/Un-tag/vlanでの暗号化
- Point-to-PointまたはAny-to-Anyの接続性

L2.5/L3ネットワーク(IP/MPLS/SR)

- Hop-by-Hopでの暗号化
- 上位IP/MPLS/SRレイヤはシームレス
- 各HopでL2.5/L3トラフィックのDrop/Add可能

L2 onlyだとイマイチ使い勝手が良くない。。



© 2026 Nokia

MACsec enhanced(ANYsec) - overview

コントロールプレーン

Encapsulate MKA in UDP and IP (MKAoIP)

- UDP: 宛先のルーターは(設定された)UDPポートでMKAoIPパケットを認識
- L3マルチホップMKAをサポート

データプレーン

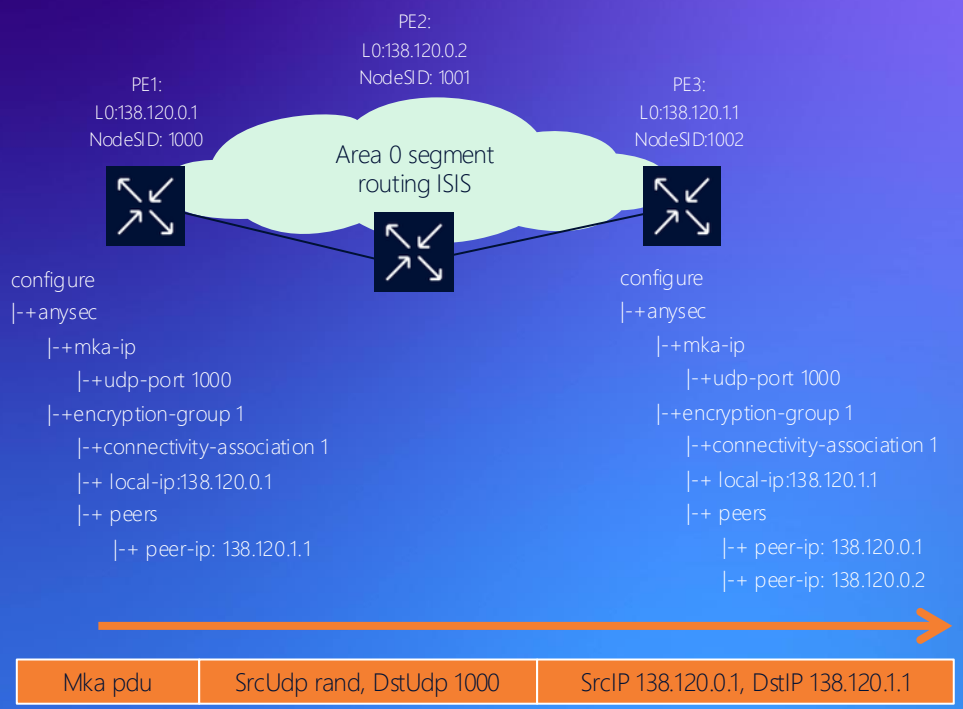
- MACsecヘッダの位置をパケットのより深い位置に置き、MPLSラベルやSRv6ヘッダをクリアに保つ
- それにより途中経路のルーターは暗号化を意識せずにパケットの転送が可能
- GCM-AES-256 / GCM-AES-XPN-256

Full description available on the public IEEE website: macsec enhanced white paper v5
https://grouper.ieee.org/groups/802/1/files/public/docs2026/new-bidgoli-macsec-enhanced-0226-v02.pdf



© 2026 Nokia

MKA over IP/UDP



- MACSec key agreement over IP/UDP
- L3NW上でのマルチホップMKAを実現
- MKA IP, source 及び destination IP address は “local-ip” と “peer-ip”により設定

```
No.   Time     Source      Destination  Protocol  Length  Info
   48 23.940…  1.0.12.2    1.0.12.1     EAPOL-…   152     Live Peer List, ICV Indicator

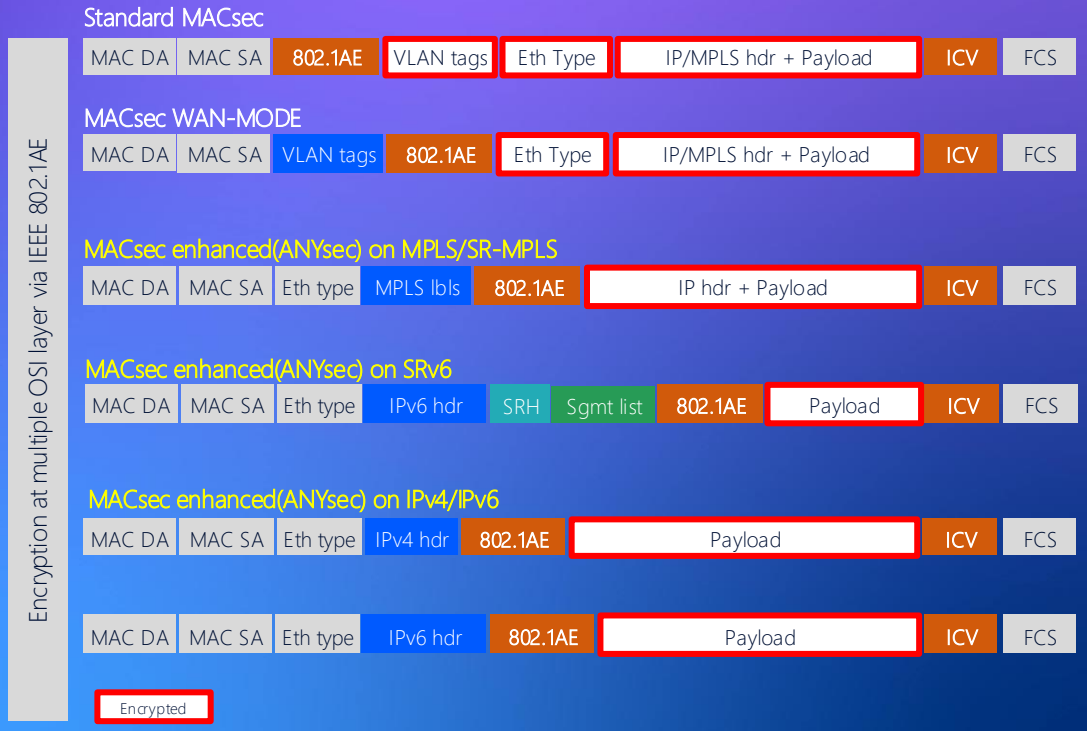
Frame 48: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface ens16, id 0
Ethernet II, Src: Nokia_74:9c:1c (9c:e0:41:74:9c:1c), Dst: Nokia_03:90:da (a8:24:b8:03:90:da)
Internet Protocol Version 4, Src: 1.0.12.2, Dst: 1.0.12.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 138
    Identification: 0x1b4f (6991)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: UDP (17)
    Header Checksum: 0x4551 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 1.0.12.2
    Destination Address: 1.0.12.1
User Datagram Protocol, Src Port: 12345, Dst Port: 12345
    Source Port: 12345
    Destination Port: 12345
    Length: 118
    Checksum: 0x02bc [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (110 bytes)
802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: MKA (5)
    Length: 104
MACsec Key Agreement
  Basic Parameter set
      MKA Version Identifier: 2
      Key Server Priority: 16
      0... .... = Key Server: False
      .1.. .... = MACsec Desired: True
      ..11 .... = MACsec Capability: MACsec Integrity with confidentiality offset (3)
      .... 0000 0011 1100 = Parameter set body length: 60
      SCI: 00000000c8020004
      Actor Member Identifier: fec4acc4452393fadbd2852b
      Actor Message Number: 00000002
      Algorithm Agility: IEEE Std 802.1X-2010 (0x0080c201)
      CAK Name: 080f23715b6d032e111c73b24c451a03659fea215511977aaee3987fcb0fad24
  Live Peer List Parameter set
```


© 2026 Nokia

IEEE 802.1AE MACsec enhanced

- 暗号化対象領域を柔軟に設定可能
- L2 / L2.5 / L3ヘッダを平文のまま 維持可能
  - MPLS / SR-MPLS
    MAC header, VLAN tags, MPLS labelは保持
  - SRv6
    MAC header, VLAN tags, IPv6/SRv6 Hdrは保持
  - IPv4/IPv6
    MAC, VLAN tags, IP headerは保持
- MACsec Enhanced（ANYsec）のIEEEでの標準化を提案中

https://grouper.ieee.org/groups/802/1/files/public/docs2026/new-bidgoli-macsec-enhanced-0226-v02.pdf



トランスポート Encryption タイプ

Bulk/Tunnel単位 or サービス単位



Bulk/Tunnel Encryption

- MACsec Per Port or VLAN Encryption
- Per LSP Encryption (Segment Routing)

Per Service encryption

- Every Service gets its own key distribution session and encryption key
- Per Service Encryption

Hybrid

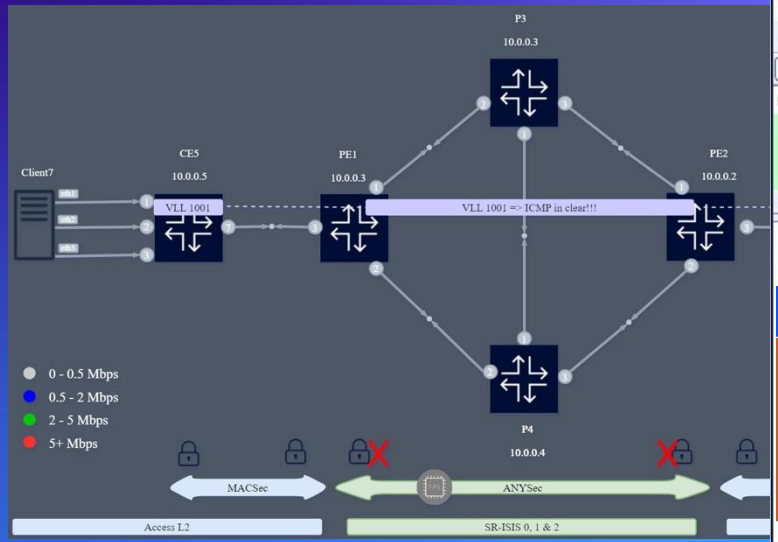
- On same tunnel
  - VPRN1 gets its own key distribution session and encryption key
  - VPRN2 and EPIPE3 are encrypted with a 2nd key distribution session and encryption key

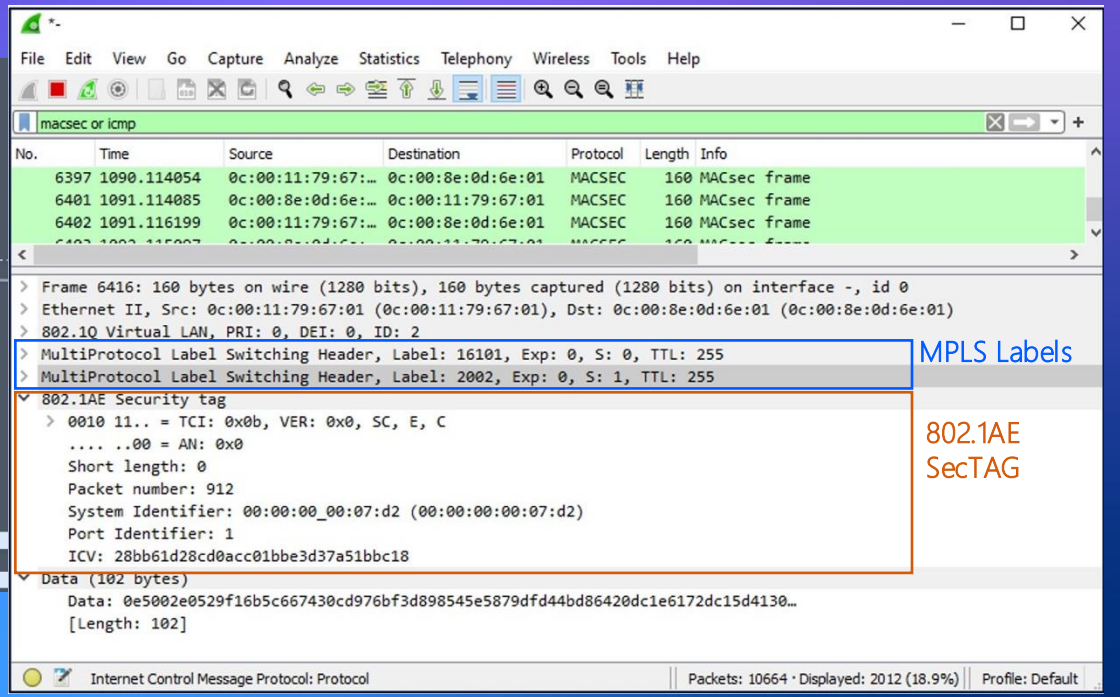
© 2026 Nokia

MACsec enhanced 実装例

on SR-MPLS　Container Lab上でのEmulation

https://github.com/srl-labs/sros-anysec-macsec-lab





© 2026 Nokia

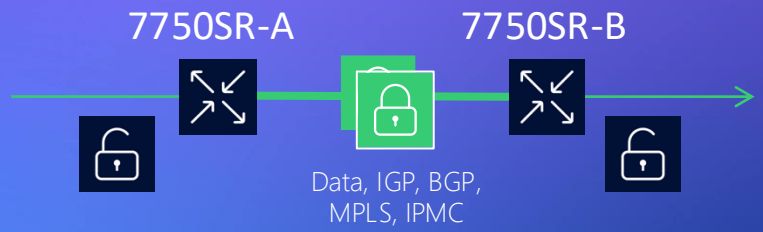
MACsec enhanced Nokiaでの各プラットフォームのRoadmap

汎用プロセッサでも実装可能に

	Nokia FP5 NP プラットフォーム	Broadcom Qumuran3 プラットフォーム	Broadcom Jericho2c+ プラットフォーム	Broadcom Jericho3 プラットフォーム
Encryption mode				
MACsec				
LAN Mode (MACsec per port)	Y	Y	Y	Y
WAN Mode (MACsec per vlan)	Y	Y	Y	Y
MPLS				
Tunnel encryption SR ISIS, OSPF, OSPFv3	Y	27.3	将来対応予定	将来対応予定
Service Encryption SR ISIS, OSPF, OSPFv3 VPRN, EPIPE, EVPN RT 5	Y	27.x	28.x	28.x
SRv6				
Tunnel Encryption	将来対応予定	将来対応予定	将来対応予定	将来対応予定
Service Encryption VPRN, EVPN RT 5	26.10	28.x	将来対応予定	将来対応予定

FP5 NPプラットフォーム(7750SR)での実装例
暗号化有り・無しでの遅延比較

- 400GE インタフェース上でのラインレートトラフィックで遅延値を比較
  - Rourer-Aで暗号化、Router-Bで復号化
    0.1~0.5uSec程度の追加遅延

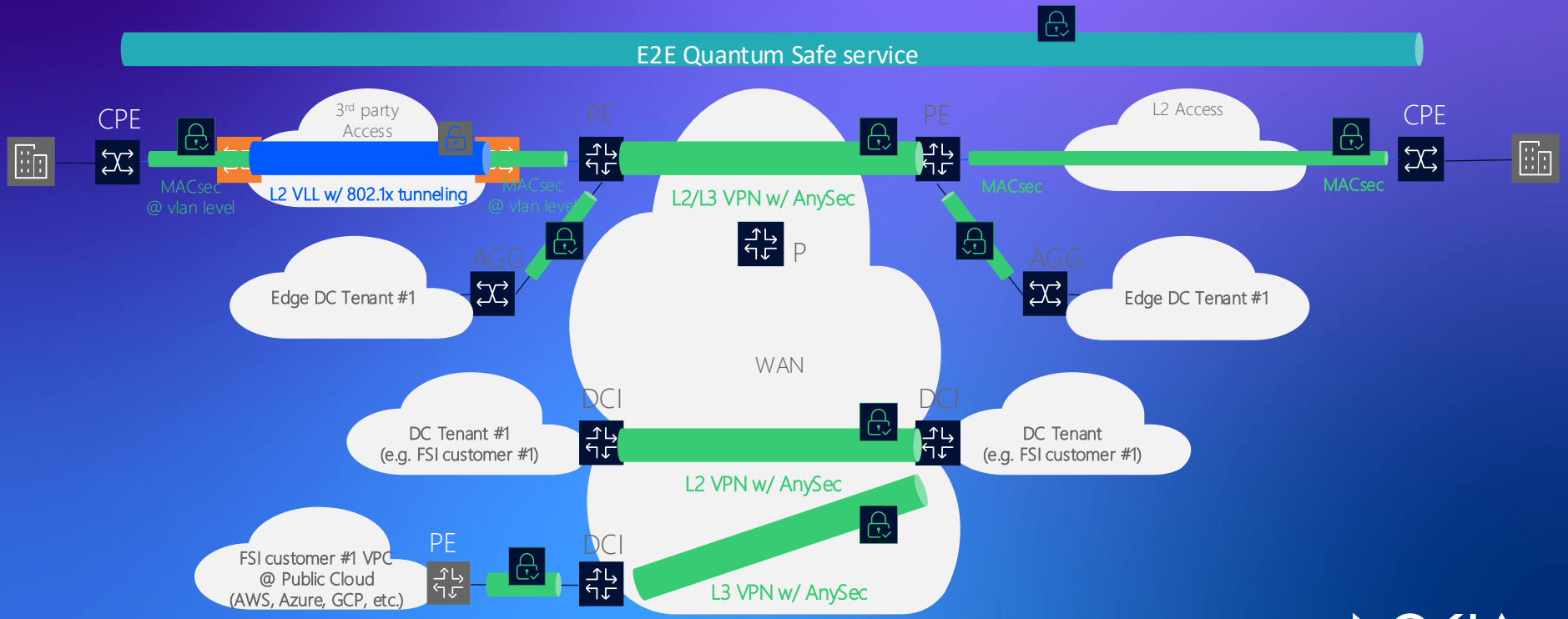


Packet size	64	1500	9000
Latency (uSec) 暗号化無し	23.25	23.24	22.88
Latency (uSec) 暗号化有り	23.35	23.47	23.4

© 2026 Nokia

導入オプション

End-to-End Quantum-Safe L2/L3サービス



© 2026 Nokia

MACsec/ANYsec key distribution

Nokia SR OSでの実装

Key chains

- キーチェーンには複数のキーエントリを設定でき、それぞれ指定した日時に有効化される。
- 各キーエントリは固有のPSKを保持する。
- PSKは手動で設定する必要がある。
- 新しいキーエントリが有効になると、新しい**MKAセッション** が生成される（PSKごとにMKAセッションを作成）
- フォールバック用途として、バックアップ用のキーエントリ（SR OS）を設定できる。
- 他ベンダーのMACsec実装との相互接続に適している。

PSK auto generate auto distribute

- IEEE 802.1AEの Distribute CAK(Connectivity Association Key配布)パラメータセット を使用する。
- 初期PSK（Pre-Shared Key）またはリカバリー用PSKとして Key Chain を利用する。
- 初期PSKは、自動生成されるPSKの配布にのみ使用され、SAK（Secure Association Key）の配布には使用されない。
- 以降のPSKは、Key Server によって自動生成され、対向装置へ自動配布される。
- PSKおよびSAKの生成には、SR OSの NIST認定エントロピー(乱数生成機構) を使用する。

SR OS/FP5 NIST and Common Criteria Certification

On going efforts to certify SROS



- 24.3R3 SR OS entropy is Certified by NIST
- Minimum 256 bit of entropy



- SR OS 24.3R3 to 27.X will be FIPS-140-3 certified
- In NIST processing queue
- NOKIA E5 (MACsec) IS CAVP certified



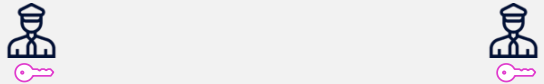
- SROS 24.10R3 NIAP certified
- SROS 27.x planned for EAL3+

© 2026 Nokia

自動化されたpre-shared key management

MACsec/enhanceのための自動化されたPSK generationとdistribution

1. 初回のみ、セキュリティ管理者がKey Chainに事前共有鍵（PSK）を登録



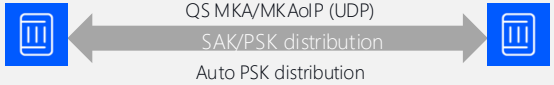
2. 初期PSKを利用して、MKAまたはMKA over IP（UDP）による量子安全鍵配布セッションを確立する



3. 以降のPSKは、SR OSが備えるFIPS/NIAP認証済み・Quantum-Safe対応乱数生成機能により自動生成される



4. MKA/MKAoIP(UDP)によりSAK又はPSKを配布



5. 新たに配布された CAK および CKN は、ノードの再起動後も CAK を保持できるよう、ルーター内に安全な方法で保存される

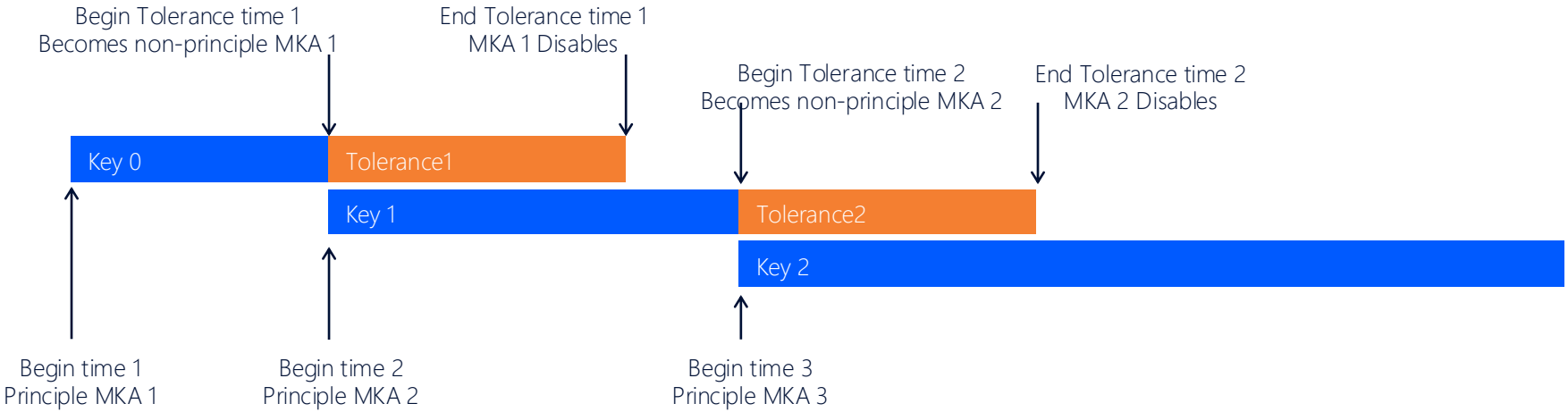


6. ユーザーが設定したタイマーに基づいて、新しい PSK が定期的に自動生成され、ネットワーク内のピアへ配布される



© 2026 Nokia

Keychain Tolerance



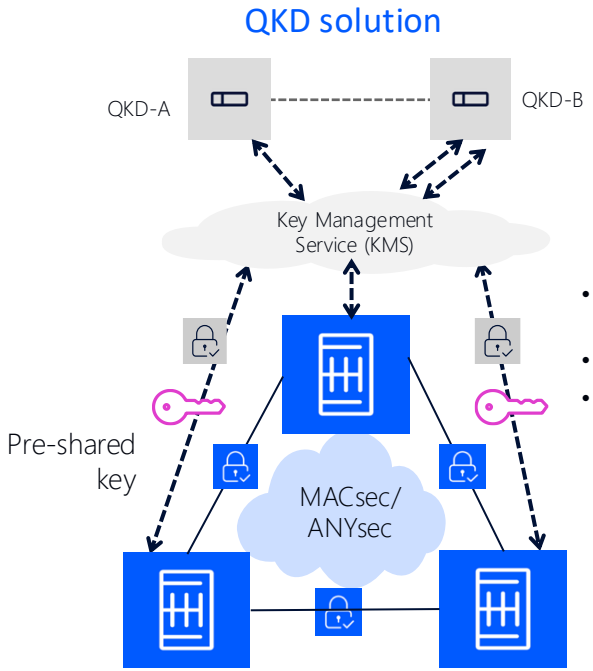
© 2026 Nokia

QKD entropy distribution (Roadmap)

MACsec, ANYsec PSK generation via QKD

PSK generation via QKD or KMS

SAK can be generated from PSK



- Router request keys from KMS using ETSI 014 and HTTPS
- KMS provides PSK via HTTPS with PQC
- If Router detects that KMS is down, it will switch back to local auto-gen auto-distribute.

© 2026 Nokia

導入ユースケース







マルチテナント (VPN services)
Segment Routing (SRv6/SR-MPLS)

IP/MPLS**及び**SR-MPLS **トランスポート**
Redundancy**と**Resiliency
レガシーサービス (EPIPE, CPIPE)

Large FAT**パイプ** (100/400/800 GE)
AI/GPUaaS **トランスポート**

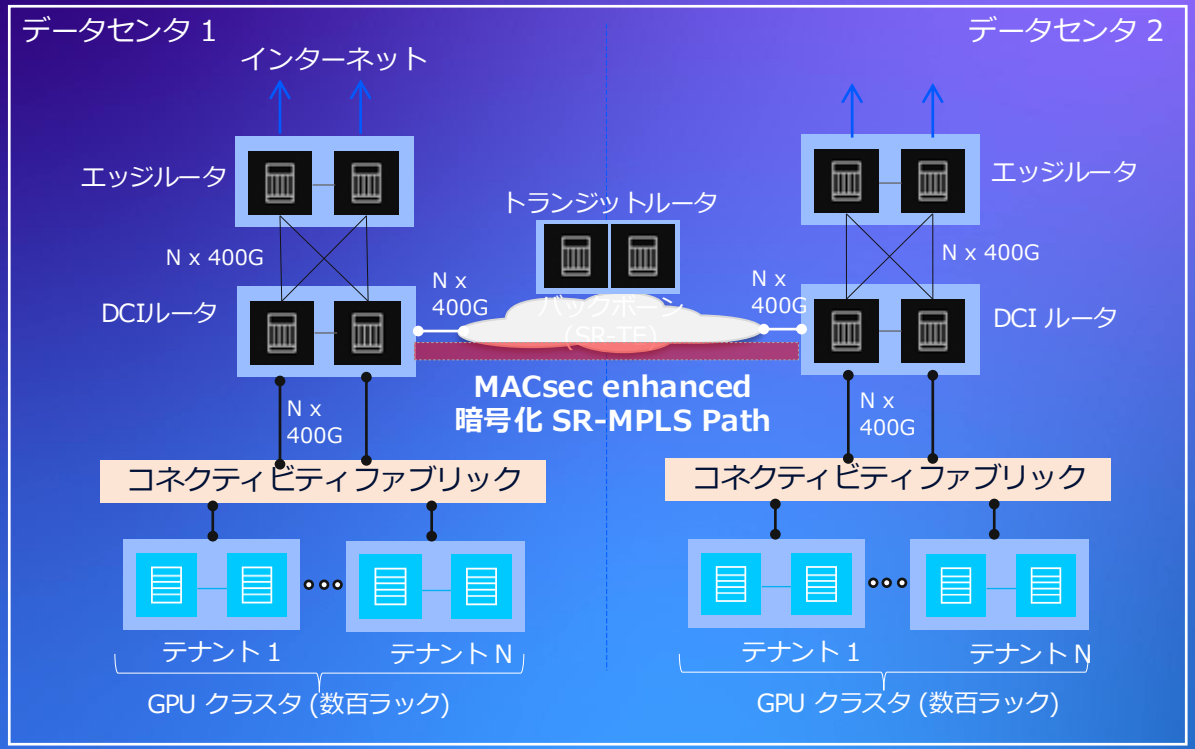
End-to-end encryption for any OSI layer with existing hardware

Ease of enabling security on existing services or transport

Security respecting existing SLA
No loss in latency and throughput

© 2026 Nokia

導入事例: US AI Cloud (GPUaaS) – DC 間接続



サービス内容

- **GPUaaS、ストレージなど**
- **初期導入は 400G、将来的に800G**
- **セキュアで暗号化通信が可能なデータセンタ相互接続サービス**

DC 相互接続ルータ要件

- DC 相互接続ルータは以下のサポートが必要:
  - VXLAN, e/iBGP, BGP-EVPN, BGP RR
  - MPLS, セグメントルーティング, QoS, NETCONF/YANG
- バックボーン経由の e2e 暗号化用の ANYSEC
- スケール: 大規模 VXLAN トンネル

© 2026 Nokia

まとめ

- MACsec enhancedによりover L2.5/L3でのoverlay
  低遅延/高帯域暗号化を実現、標準化提案中
- 汎用NP(BRCM J2+/Q3/J3)で実装可能、他NW機器ベンダーへの実装の広がりを目指す
- Key autogeneration/distributionを実装、QKDソリューション/KMSとの連携等他方式にも対応予定
- CSPでのBusiness VPNサービスの拠点間接続やGPUaaS事業者でのDC間接続など導入が始まっている

© 2026 Nokia


NOKIA