



Securing Data in Motion

Uli Schlegel

30th of October 2015

ADVA Optical Networking Today



Mission

Our MISSION
is to be
the trusted partner
for innovative
networking solutions
that ADVANCE
next-generation
networks for cloud
and mobile services.



Ulrich Dopfer
CFO

Brian Protiva
Co-Founder & CEO

Christoph Glingenner
CTO

Key Facts

Our NUMBERS

1.500 employees
€339* million revenue
20 years of innovation

*annual 2014

Our CUSTOMERS

Hundreds of carriers
Thousands of enterprises

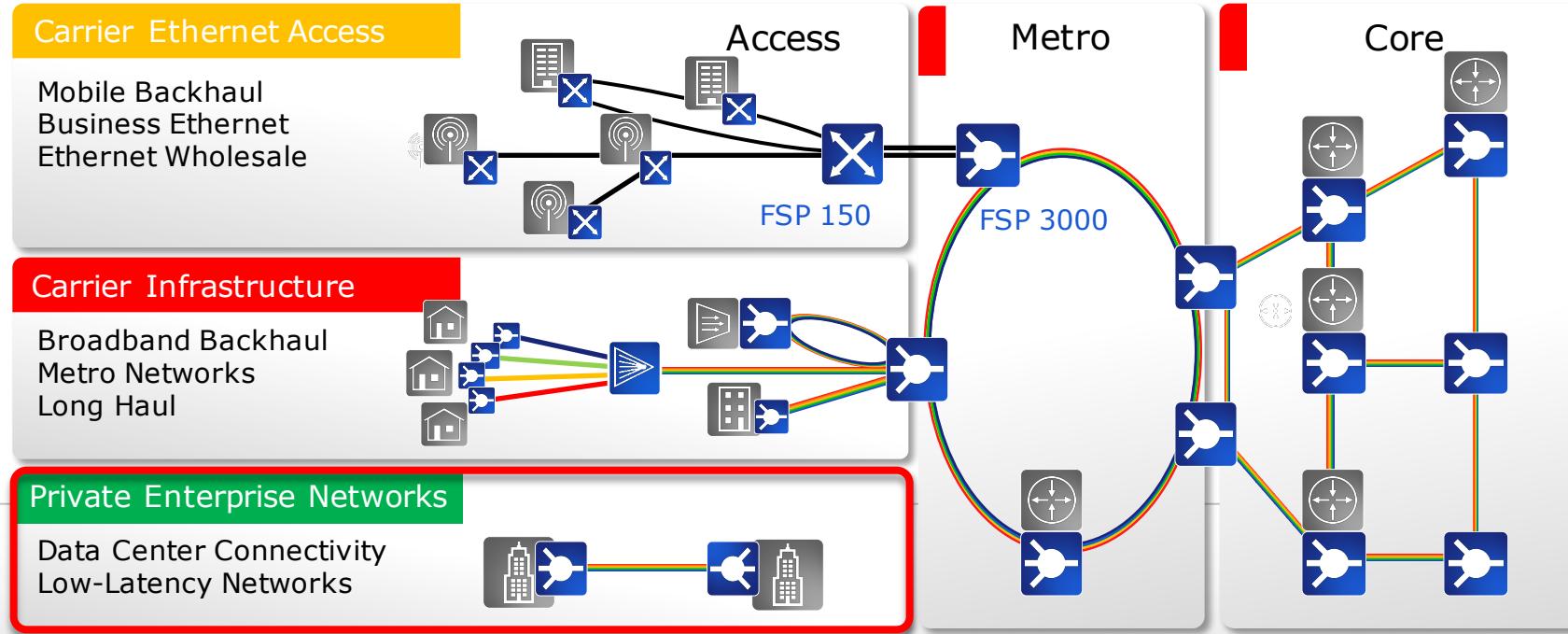
Our QUALITY

TL 9000, ISO 14001
Award-winning
supply chain

We bring differentiation, quality and ease-of-use to next-generation networks

Our Solutions Overview

FSP Service Manager



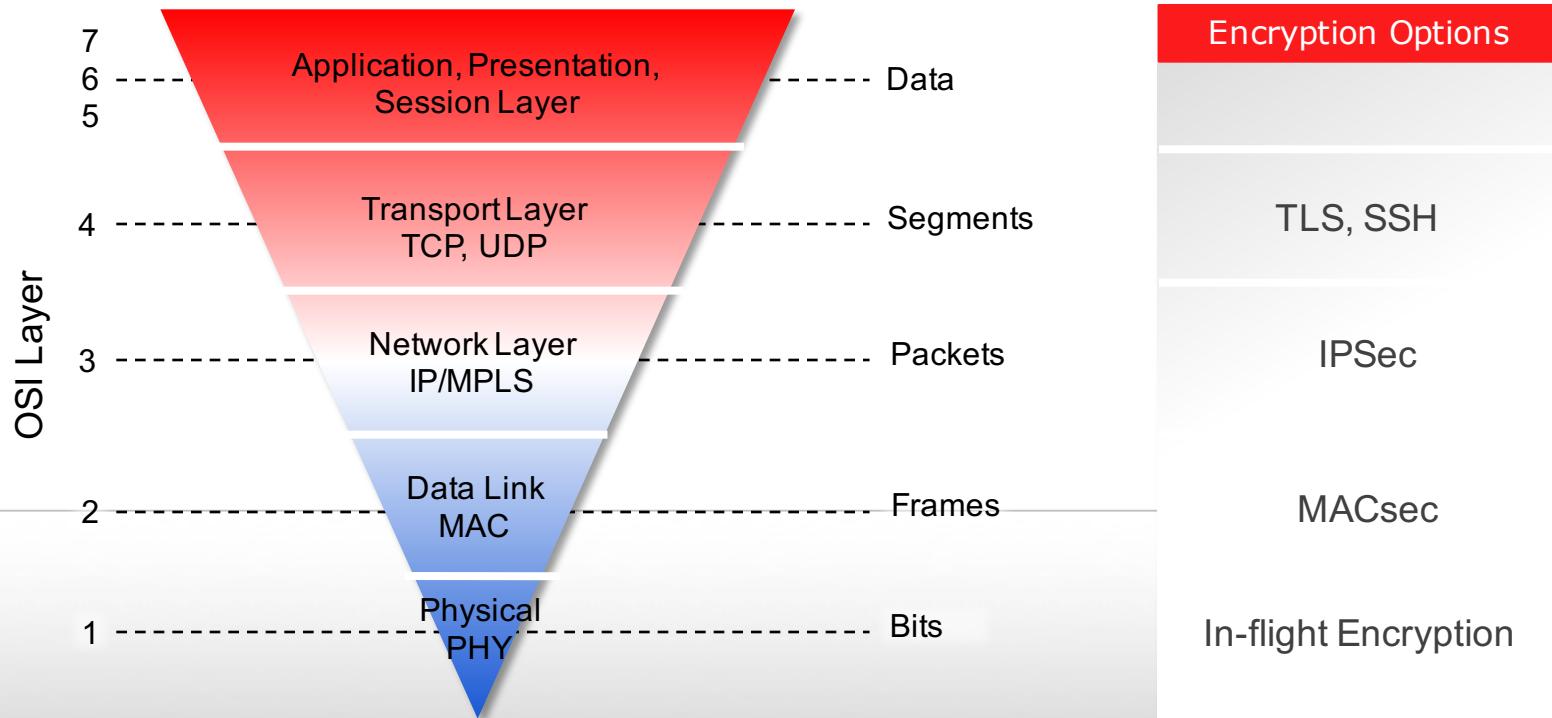
Automated service delivery and assurance from access to core

Network Encryption



Today and tomorrow

Securing Data in Motion



Optical transmission security

Speed of Encryption

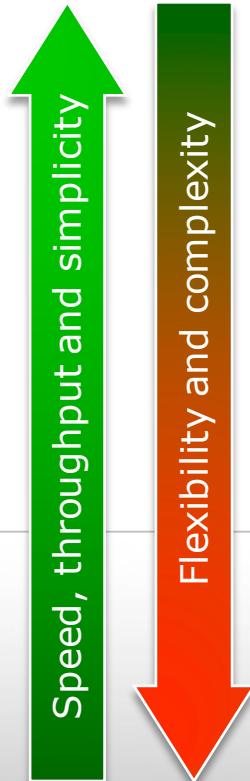
xWDM based Encryption



Ethernet based Encryption



IPsec based Encryption

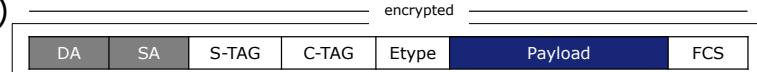


High Speed Encryption Modes



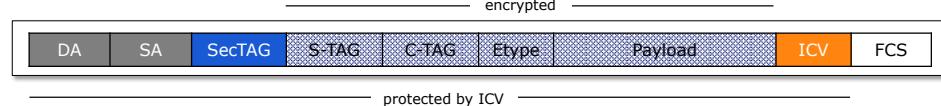
- Point-to-Point,
- Protocol/ I/F agnostic (ETH, FC/IB, Sonet/SDH)
- Integrated Solution with lowest latency

Bulk Mode (0 Bytes)



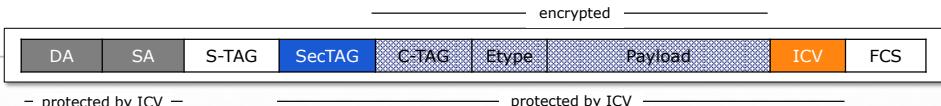
- Hop-by-Hop only
- Pure Ethernet based
- Overhead increase

MACsec +32 Bytes



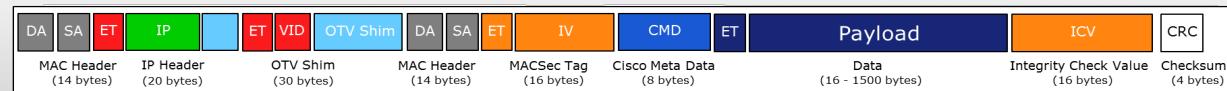
- **End-to-End PtP or Multi-Point**
- Pure Ethernet based
- Overhead increase

MACSEC+32 Bytes



- Huge overhead
- IP VPN Services
- Cisco Nexus

Cisco Overlay Transport Virtualization (OTV) +82 Bytes



ConnectGuard™ Ethernet Solutions



- Advanced MACsec transformation
- IEEE 1588 times stamping on MACsec ports
- Same L2 OAM, TM and PM features as GE114
- L3 capabilities
- SDN enabled

- Advanced MACsec transformation
- IEEE 1588 times stamping on MACsec ports
- Same L2 OAM, TM and PM features as the XG210

ADVANCED MACsec Transformation

MACsec with VLAN bypass



Unencrypted Frame



+32 Bytes

encrypted

Standard MACsec Format



protected by ICV

encrypted

Single VLAN bypass MACsec Format



- protected by ICV -

protected by ICV

encrypted

Double VLAN bypass MACsec Format

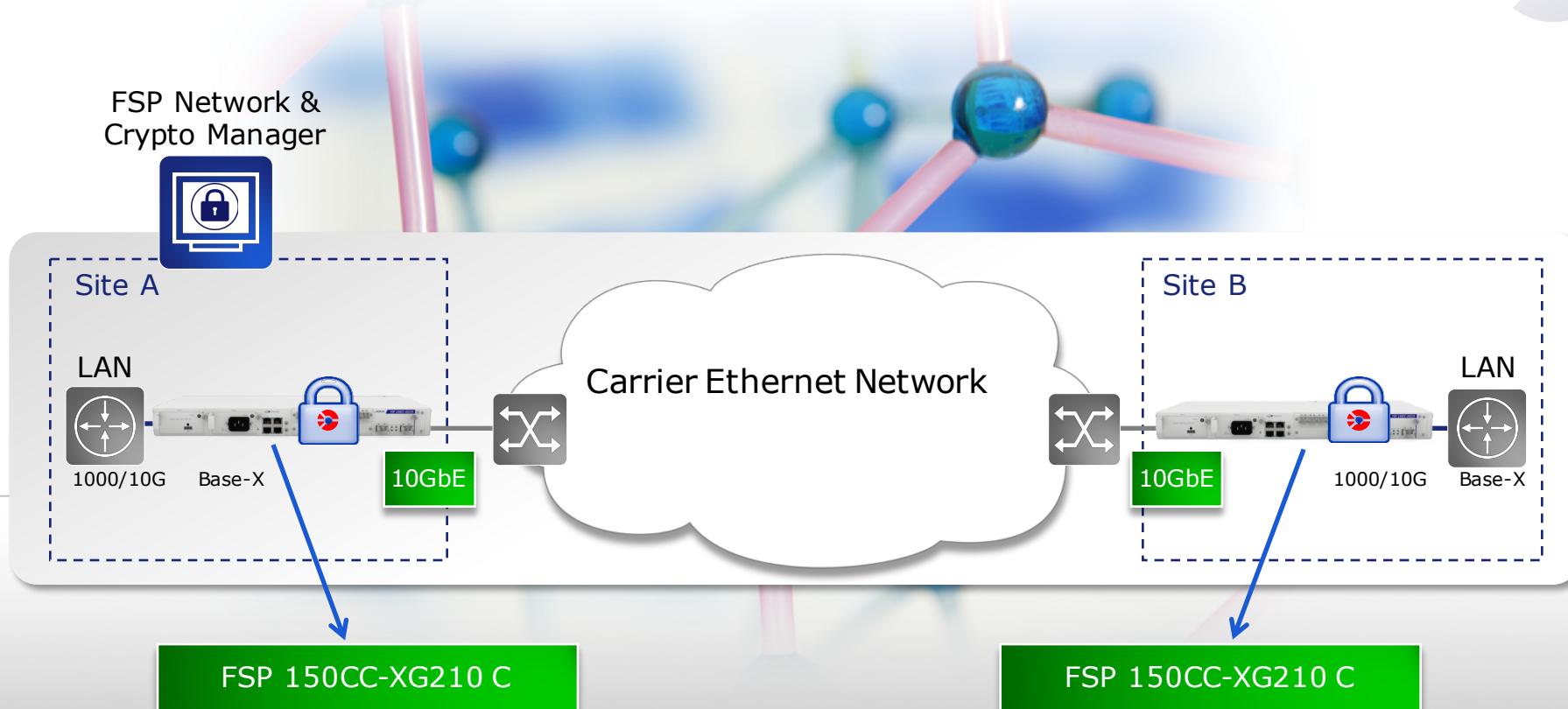


- protected by ICV -

protected by ICV

Encryption over L2 Carrier Networks

1Gbit - 10GbE Services Port based Point to Point



FSP 3000 Enterprise

Lowest power consumption

- More than 50% lower power consumption compared to competitors

Lowest space requirement

- 50% higher rack space efficiency

Lowest latency transport

- Latency optimized transponder cards for synchronous enterprise applications

Lowest TCO

- Most cost effective system in the market
- Simple and straight forward system architecture allows for fast and easy setup and maintenance

Leading feature set

- Support of all enterprise protocols and I/Fs:
FICON, 1/2/4/8/10/ 16G FC, Video
GbE, 10/40/100GE, RoCE, IB (SDR, DDR, QDR), 40G, 100G
- Qualifications for all major enterprise apps (e.g. IBM GDPS)
- Optical line monitoring (OLM, OTDR, OSA)
- Encryption: 1Gbit to 100Gbit seamless
- Sophisticated optical layer: ROADM, EDFAs, RAMAN, DWDM 196λ



The scalable optical transport solution



KRUNG THAI BANK PCL



Morgan Stanley



THE UNIVERSITY OF ALABAMA
UNIVERSITY OF ARKANSAS



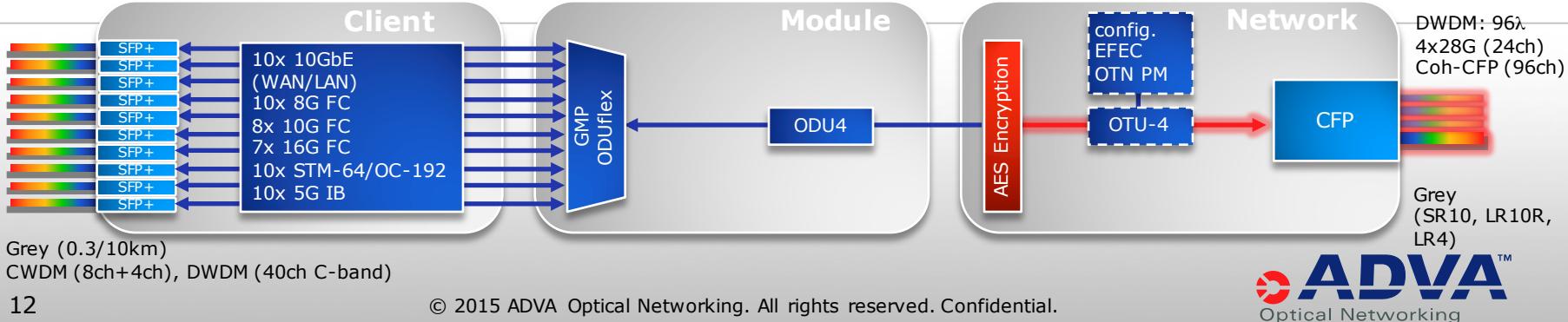
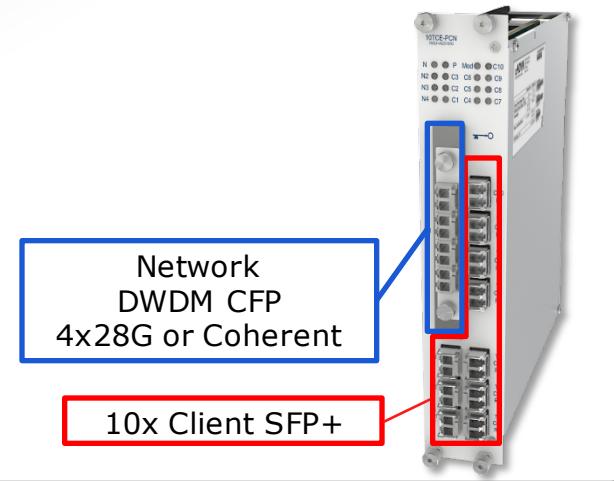
NewYork-Presbyterian
The University Hospital of Columbia and Cornell

ADVA
Optical Networking

100G Muxponder with Encryption

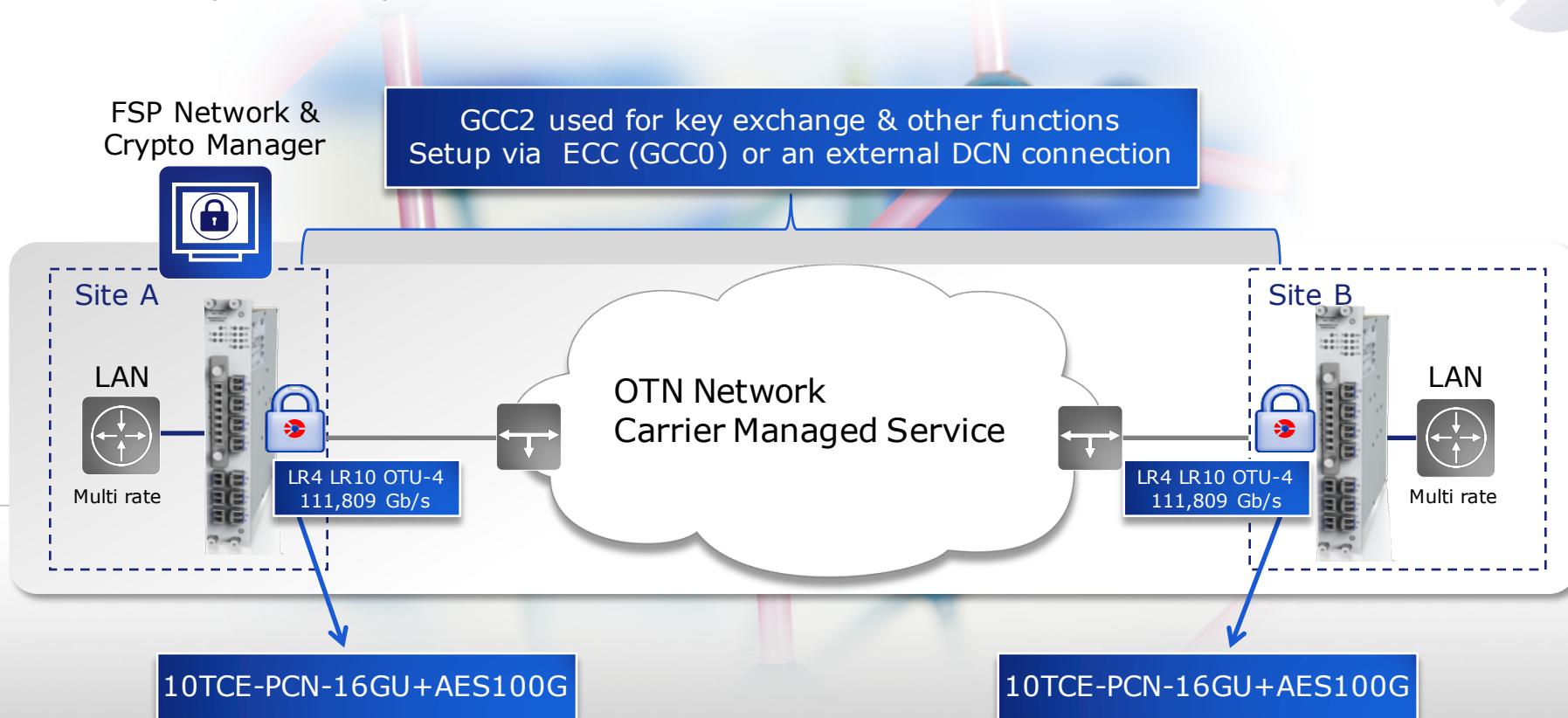
10TCE-PCN-16GU+AES100G- (BSI)

- AES256 encryption
- Next level random number generation w/ inbuilt validation
- Dynamic key exchange using PACE with 2048bit key (60/h)
- Message Authentication Code (MAC)
- Up to 10 x multi-service
 - 10GbE, STM-64/OC-192, FC8/10/16, 5G IB
 - 40GbE/100GbE via break out cable
- Client Channel Card Protection
- GFEC for 4x28 CFP, GFEC/EFEC Coh-CFP



Encryption over L1 Carrier Networks

10GbE, 40GbE, 100GbE Services

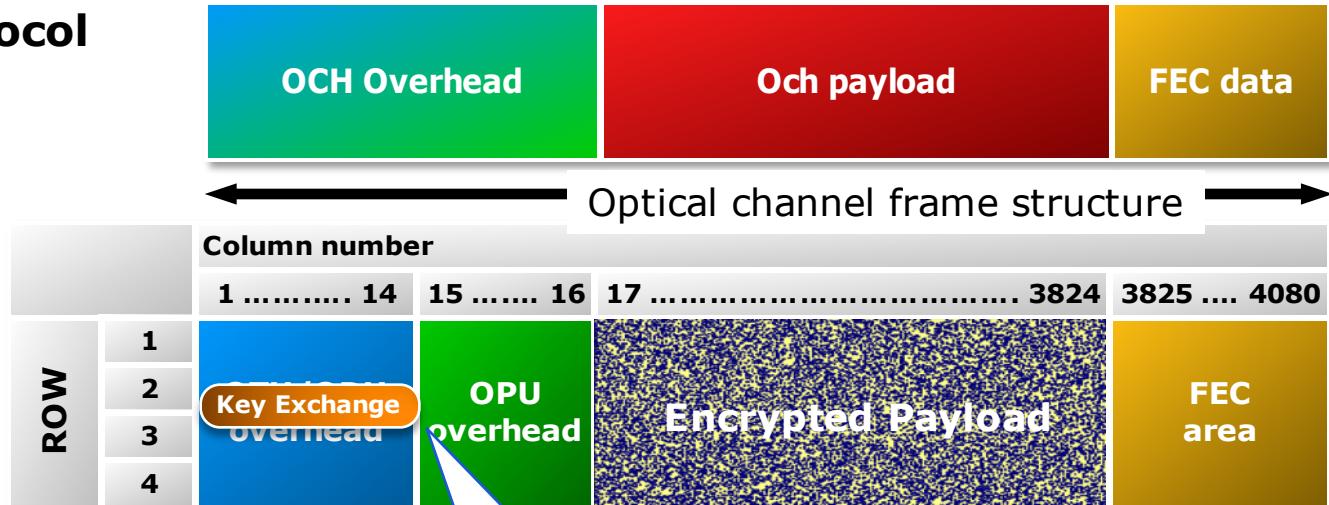


Encryption using G.709 / OTH Link Protocol

5TCE-10G card, 10TCE-100G card

5TCE-10G link protocol

- Supports
 - OTU-2
 - OTU-2e
 - OTU-2f



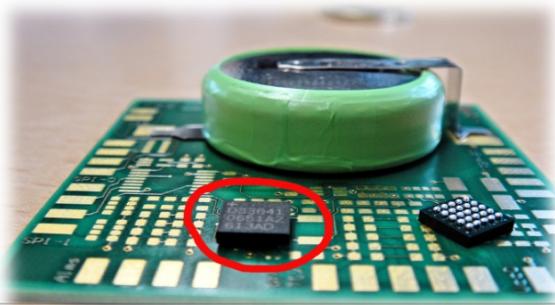
10TCE-100G link protocol

- Supports
 - OTU-4

Automatic key exchange using DH

AES 256 encrypted OPU2 payload

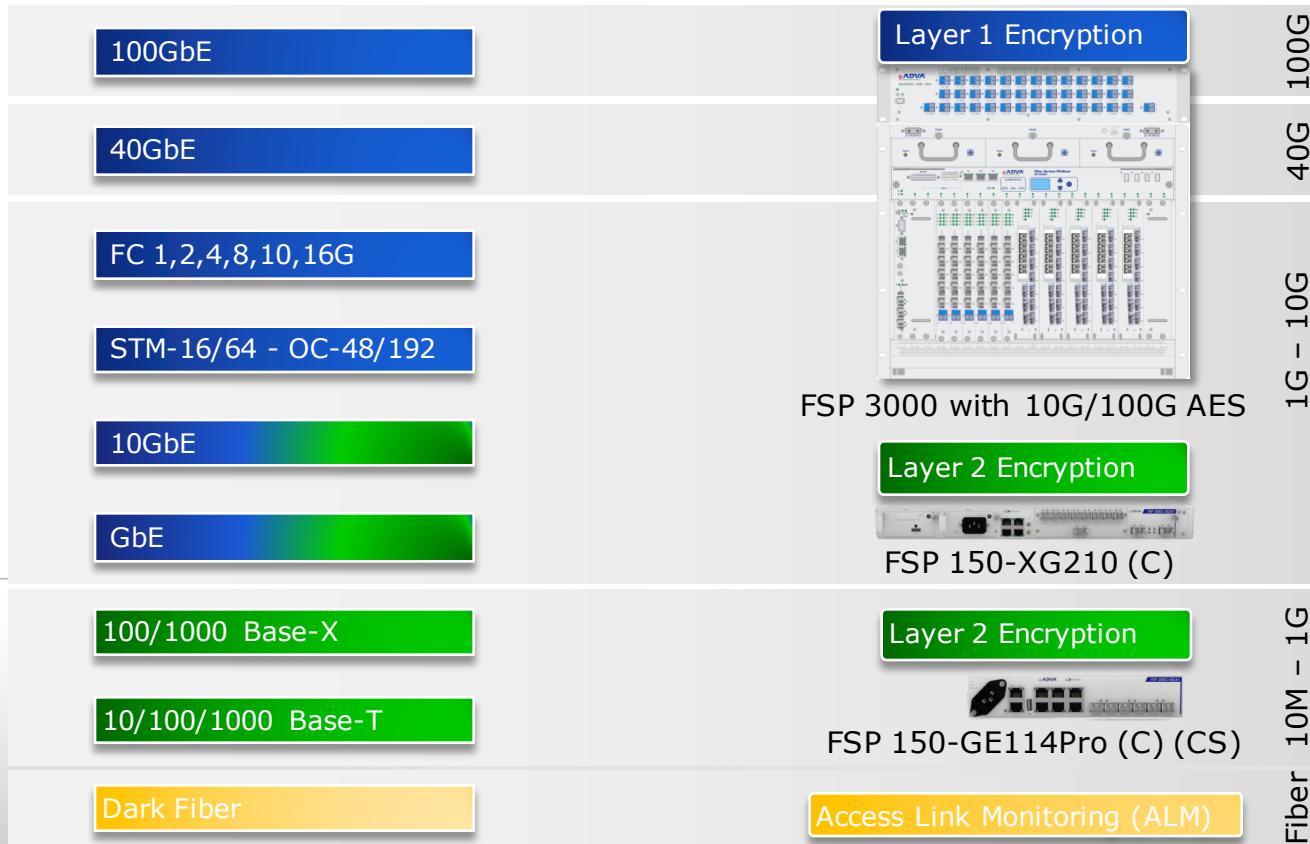
Secure Storage & Tamper Detection



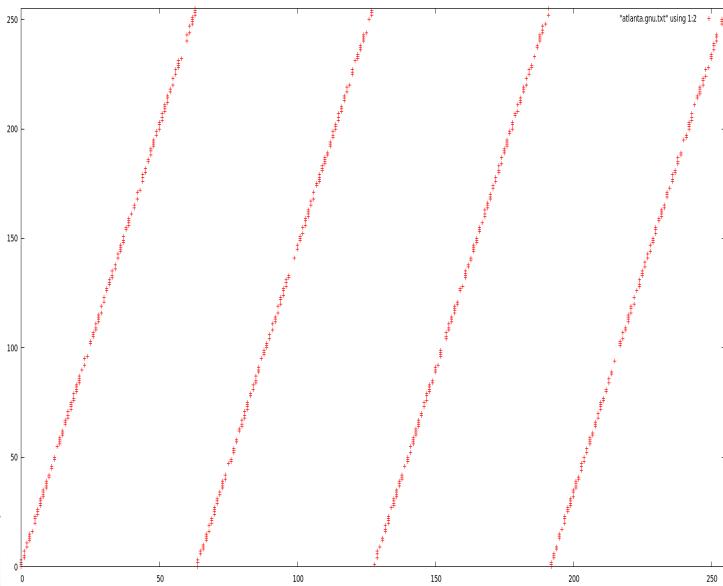
Maxim DS3641

- battery-buffered non-imprinting RAM with high-speed erase
- three digital inputs for tamper detection
- programmable temperature sensor
- crystal oscillator tamper monitoring
- voltage tamper monitor
- latching and time stamping of tamper events
- developed according FIPS 140-2 level 4

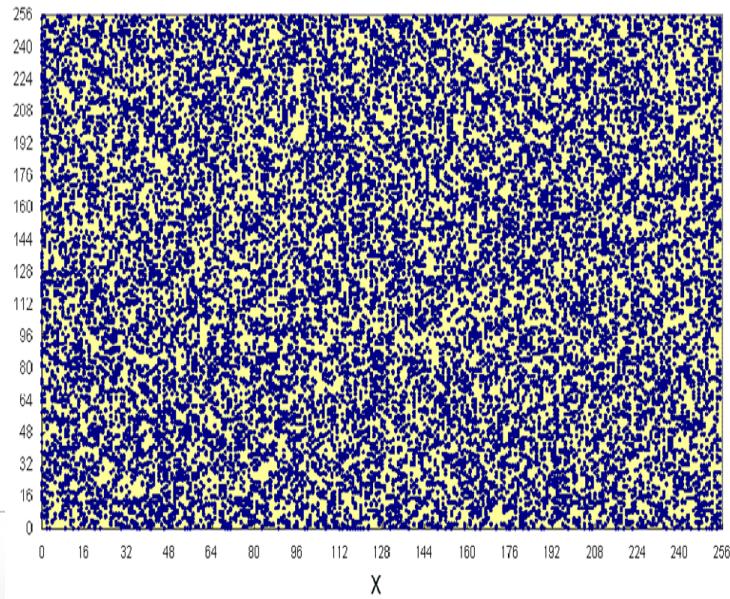
10Mbit/s to 100Gbit/s Transport Security



X-Y Plot of the RNG output



A FIPS approved RNG



The RNG used by ADVA

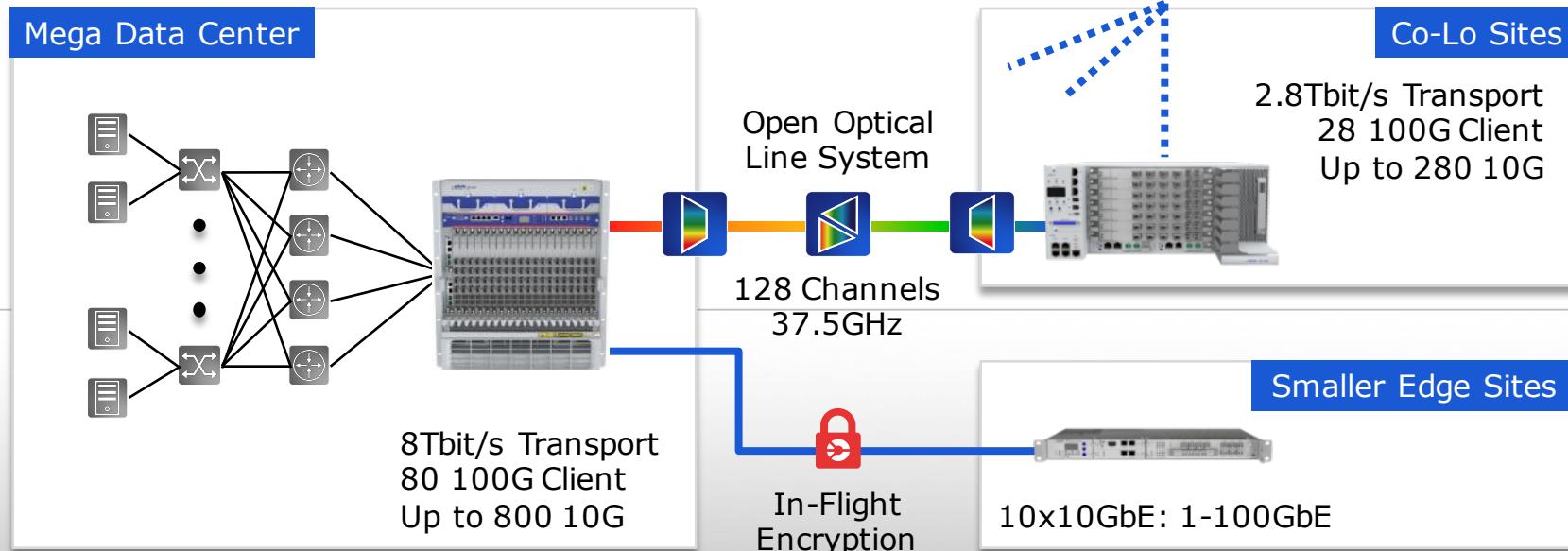
Technology Outlook



Data Center Interconnect Solution



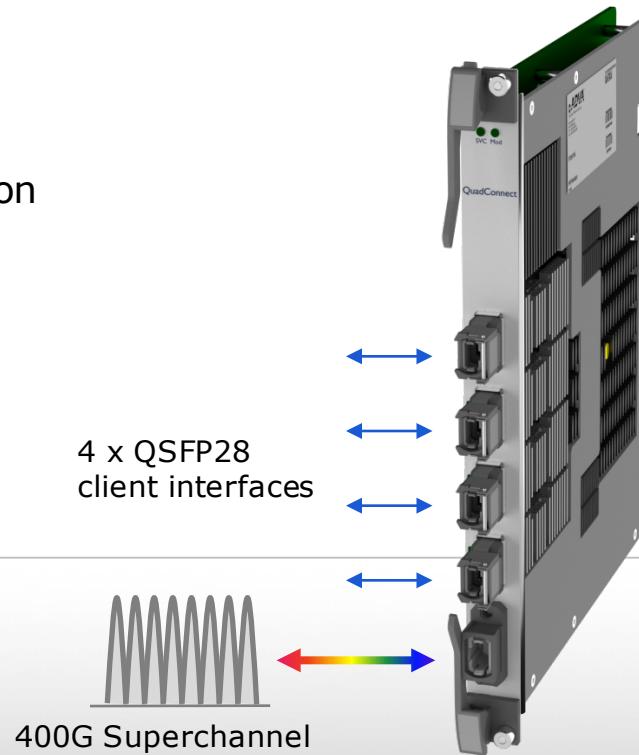
Highest fiber capacity: 25.6T to 50T
Highest density: 25.6T per 42RU Rack
Highest power-efficiency: 0.5W/Gbit/s



400G DCI Optimized module

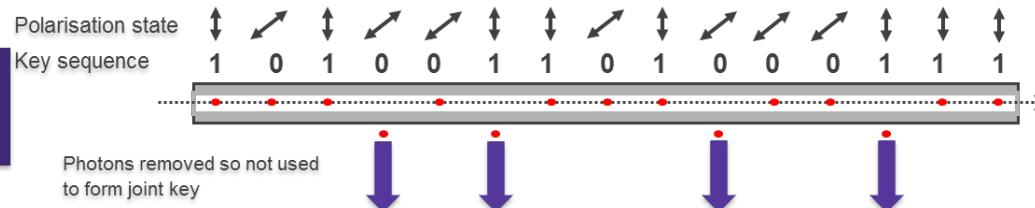
QuadConnect

- Optimized **Datacenter** Interconnect
- 1 x integrated, 400G interface
- 8 x 28GBd HOM Superchannel with direct detection
- Up to 4.8Tbit/s fiber capacity
 - Future 9.6Tbit/s
- 4 x QSFP28 client interfaces
 - 25GbE, 100GbE, OTU4, 32G FC, 128G FC
- Reach 100km
- AES 256 Encryption
- Power Consumption : typ 100W

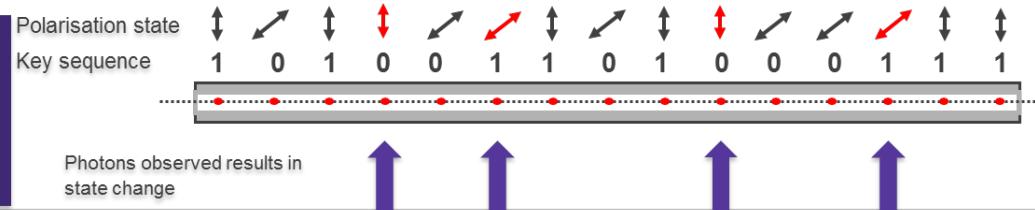


Quantum Key Distribution: Unhackable

If photon removed
it doesn't get used



If photon observed,
its state is changed
and this is
detected



Quantum mechanics has proven that the act of observing something changes its state in a non-reversible way



Thank You

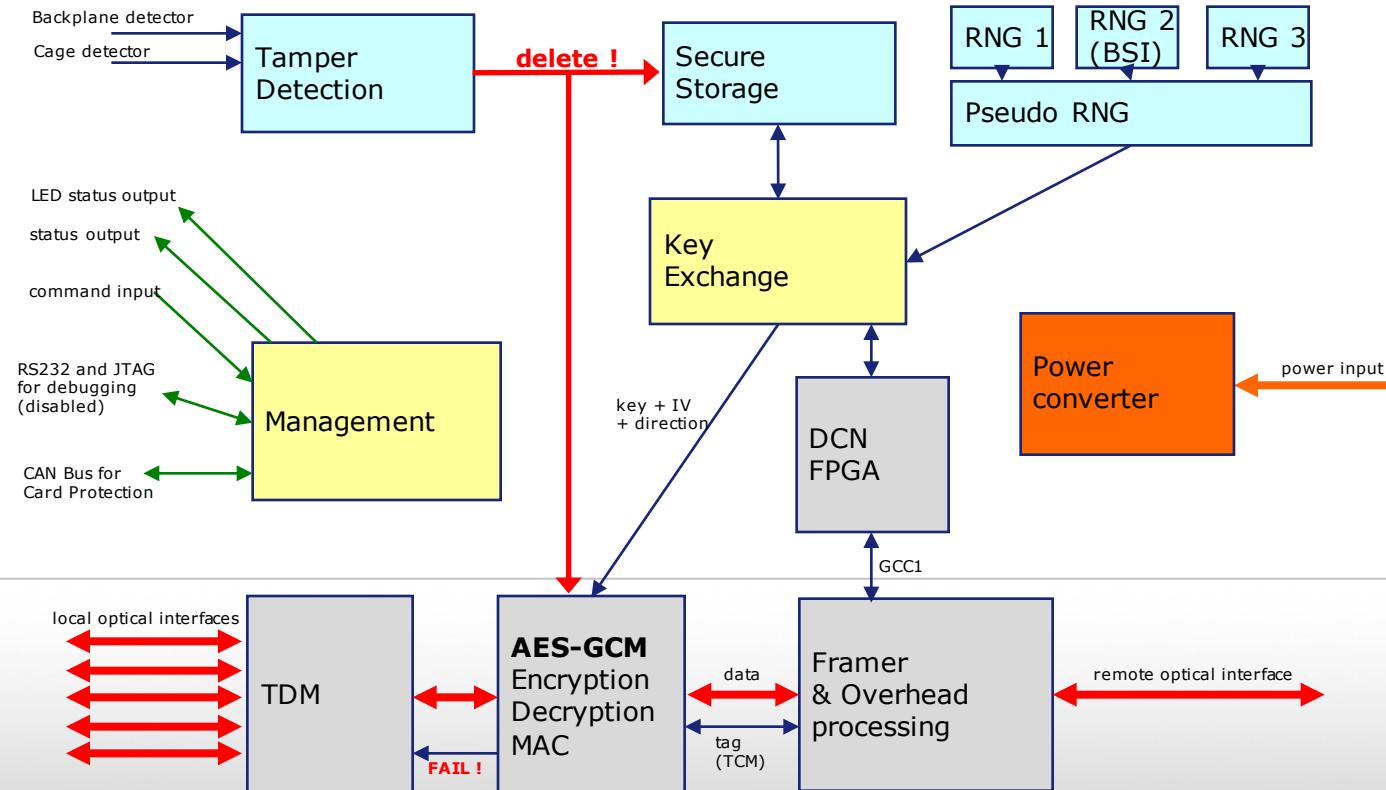


IMPORTANT NOTICE

The content of this presentation is strictly confidential. ADVA Optical Networking is the exclusive owner or licensee of the content, material, and information in this presentation. Any reproduction, publication or reprint, in whole or in part, is strictly prohibited.

The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA Optical Networking shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation.

10TCE-AES Block Diagram



World's First QKD + 100Gb/s Field Trial

