



# Security and Encryption in WDM Systems

Benedikt Moser  
October 2009

# ADVA Optical Networking

"ADVA is a **leading global provider** of xWDM **optical networking solutions** for rapid and cost effective provisioning of high-speed data, storage, voice and video services in the **Enterprise** world.."



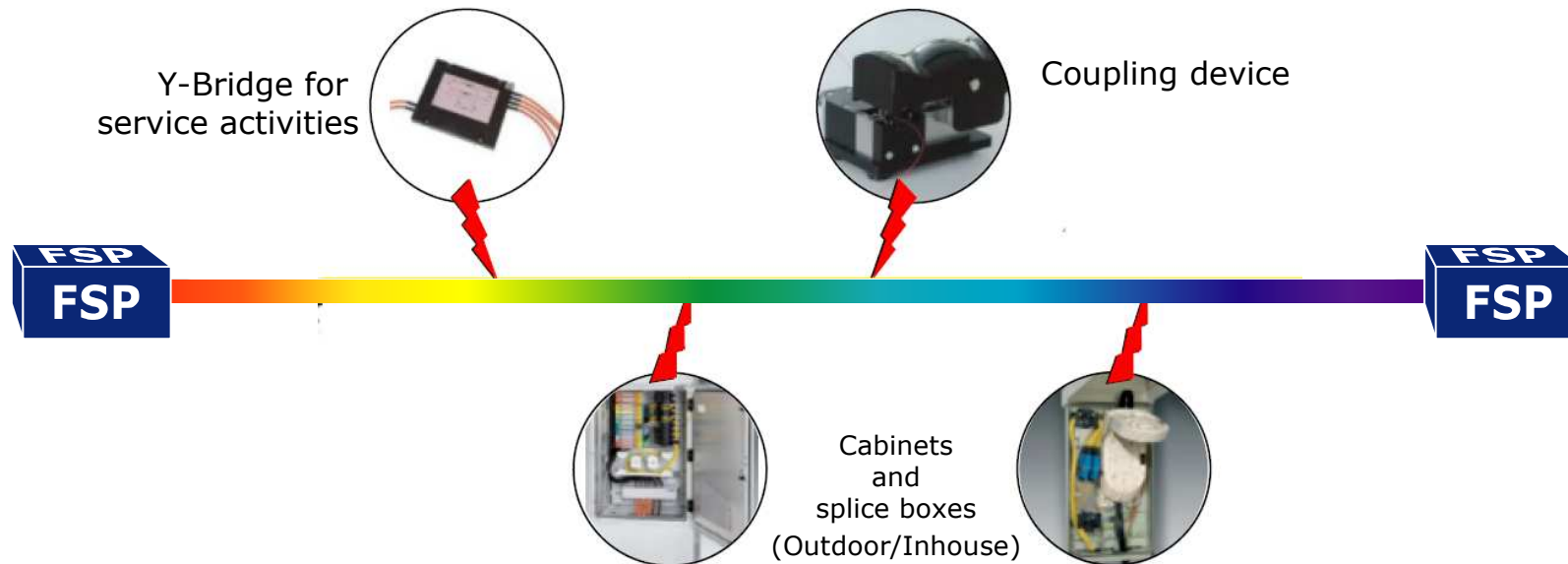
- ▶ ADVA Optical Networking
- ▶ Founded 1994
- ▶ ~ USD 300 million revenue<sup>1)</sup>
- ▶ Public company (FSE: ADV)
- ▶ > 1,000 employees<sup>1)</sup>
- ▶ Diverse global customer base
  - ▶ > 10,000 enterprises
- ▶ Market leader in Enterprise Connectivity solutions

1) 2008

**...let us show you how our solutions  
help you solving Enterprise Connectivity problems**

# Transport security

## Fiber tapping



- ▶ until recently tapping of fiber was considered as almost impossible
- ▶ DWDM and the type of data transmitted was considered as kind of encryption
- ▶ available encryption solutions did not scale beyond GbE and were very expensive

**only recently has the threat become big and the price levels low enough to have enterprises thinking about encryption**

# Transport security Solutions

- ▶ Owning dark fiber
  - ▶ Does not prevent from 3rd party intrusion
- ▶ Physical protection / Shielding of Fiber Path
  - ▶ Not economical
- ▶ Monitoring of optical performance (e.g. OLM module of the ADVA FSP)
  - ▶ Allows to detect tapping of fiber
  - ▶ No protection against reading of data
- ▶ In-flight encryption of transmitted data
  - ▶ Transmitted data is protected
  - ▶ Even reading of data does not provide meaningful content

**Different levels of protection/encryption to accommodate different requirements**



# Monitoring of optical performance

## Advance OTDR functionalities for WDM systems

October 2009

# Monitoring of optical layer performance

## Optical power tracking (OLM functionality)



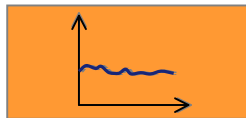
fiber cut

- ▶ fiber cut protection through software adjustable switching thresholds



fiber degradation

- ▶ alarm generation through adjustable min/max fiber attenuation thresholds



long-term effects

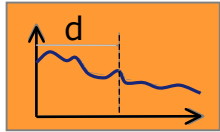
- ▶ Long term fiber performance information through integrated database



fiber intrusion

- ▶ Intrusion detection through correlation of typical power signatures

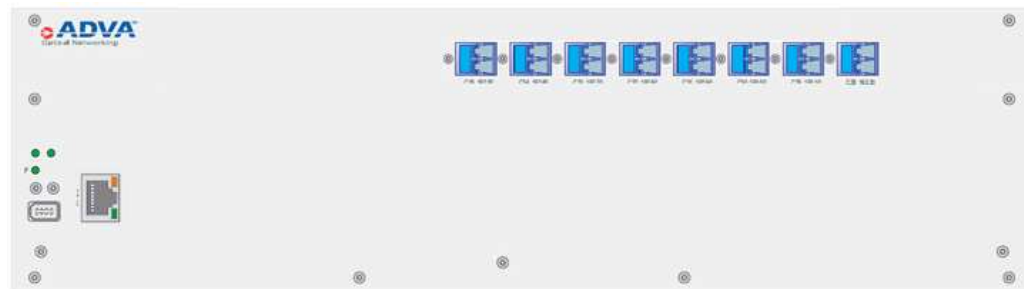
# Optical fiber fault locator- OTDR



fault location

- ▶ Geographical presentation of fiber link
- ▶ Localization of fiber splices, patch panels and fiber breaks
- ▶ **Optical ports:** 8 bidirectional OTDR ports (via 1x8 switch)
- ▶ **Resolution:** near field : ~1m; far field : ~100m
- ▶ **Management:** Integrated in ADVA node management
- ▶ **Mechanics:** Rack mountable 3HU unit
- ▶ **Availability:** Release 9.3, Q4/2009

## OTDR #1650



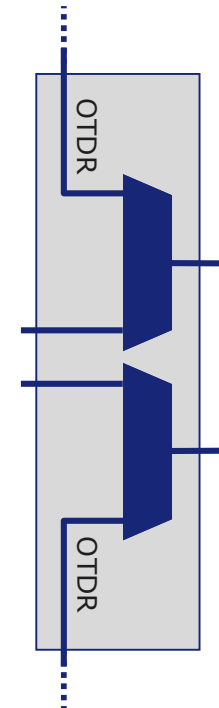
# Optical fiber fault locator

## OTFM – Filter module

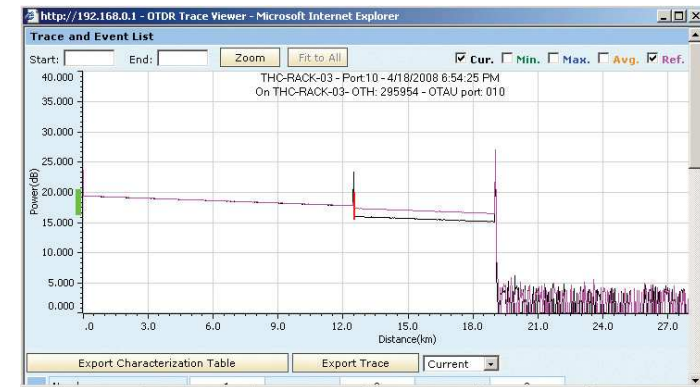
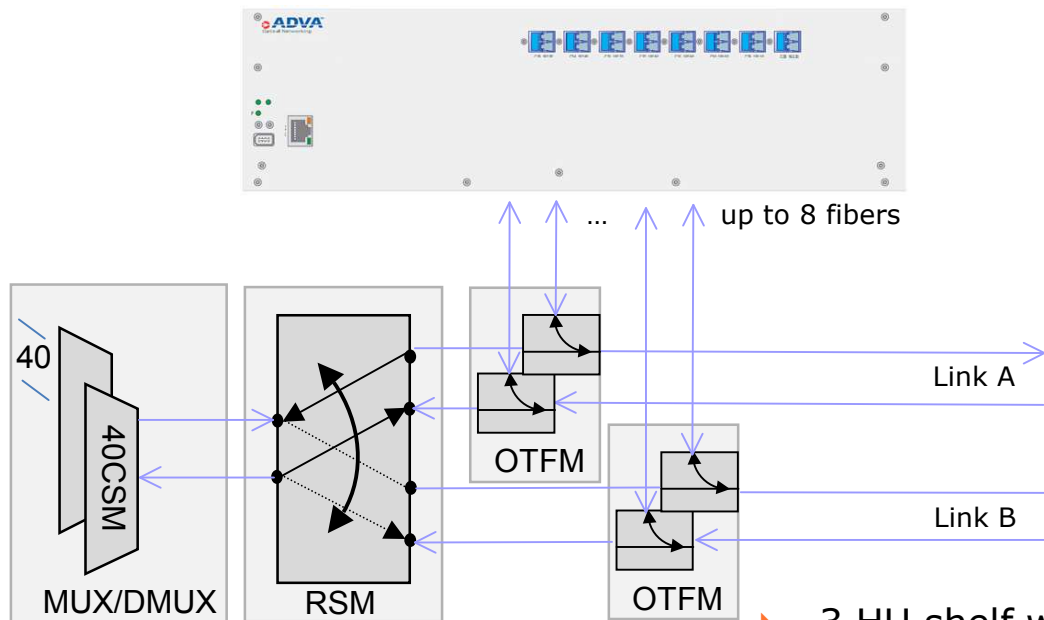


### OTFM #1650

- ▶ **Optical ports:** network, client and OTDR ports LC-PC
- ▶ **Internal:** dual very high isolation edge filters w/  $\sim 1$ dB loss
- ▶ **Features:** designed for OTDR measurements
- ▶ **Availability:** Release 9.3, Q4/2009



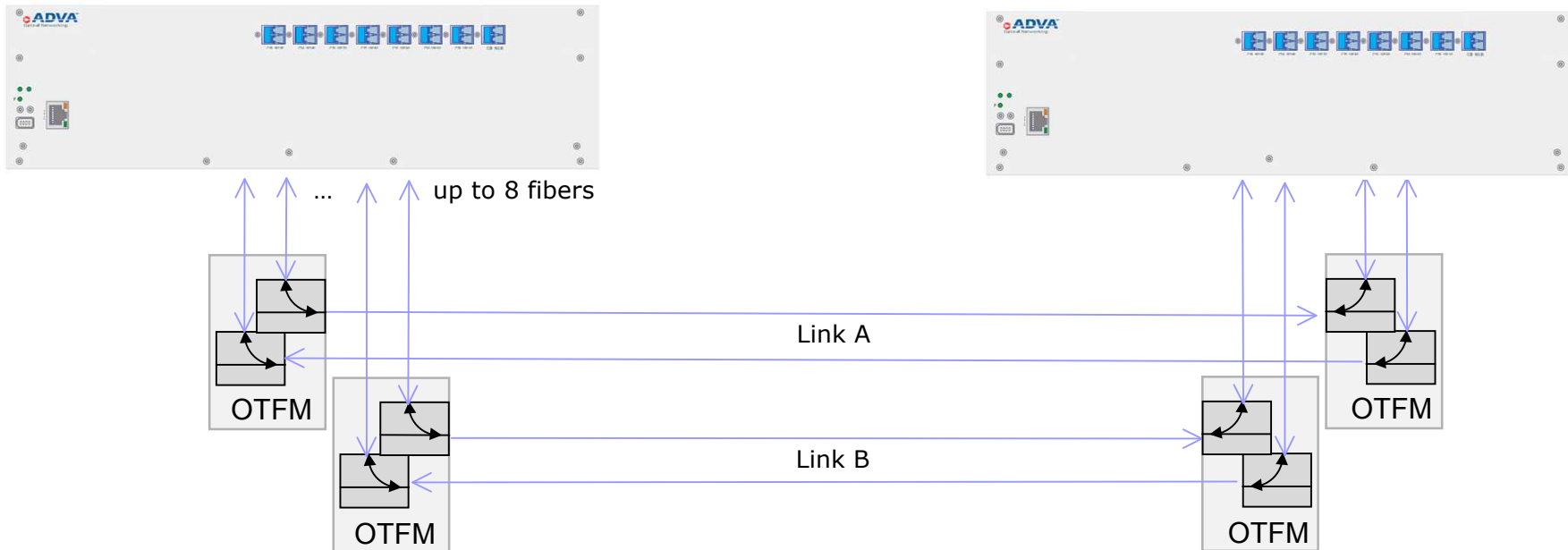
# Optical monitoring OTDR – single ended



- ▶ 3 HU shelf with management integration into ADVA EMS
- ▶ 8 local ports for fiber monitoring at 1310 or 1625 nm
- ▶ Near end mode (<1km, resolution 1m) and far end mode (<100km, resolution, 100m)
- ▶ Single ended operation

# Optical monitoring

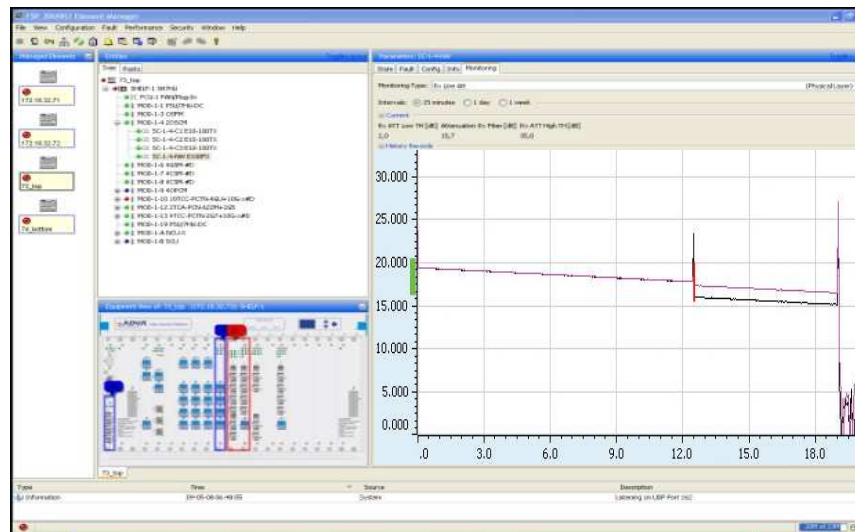
## OTDR – Dual Ended



- ▶ Dual ended operation with result correlation
- ▶ Near end mode (<1km, resolution 1m) and extended far end mode (<200km, resolution, 100m)
- ▶ Feature for later release (R 10.1)

# OTDR - Software features

- ▶ OTDR scan 'On demand' via management
- ▶ OTDR scan scheduled via management (hourly, daily, monthly)
- ▶ Database for scan results (stored on local PC)
- ▶ Graphical Integration within ADVA element Manager



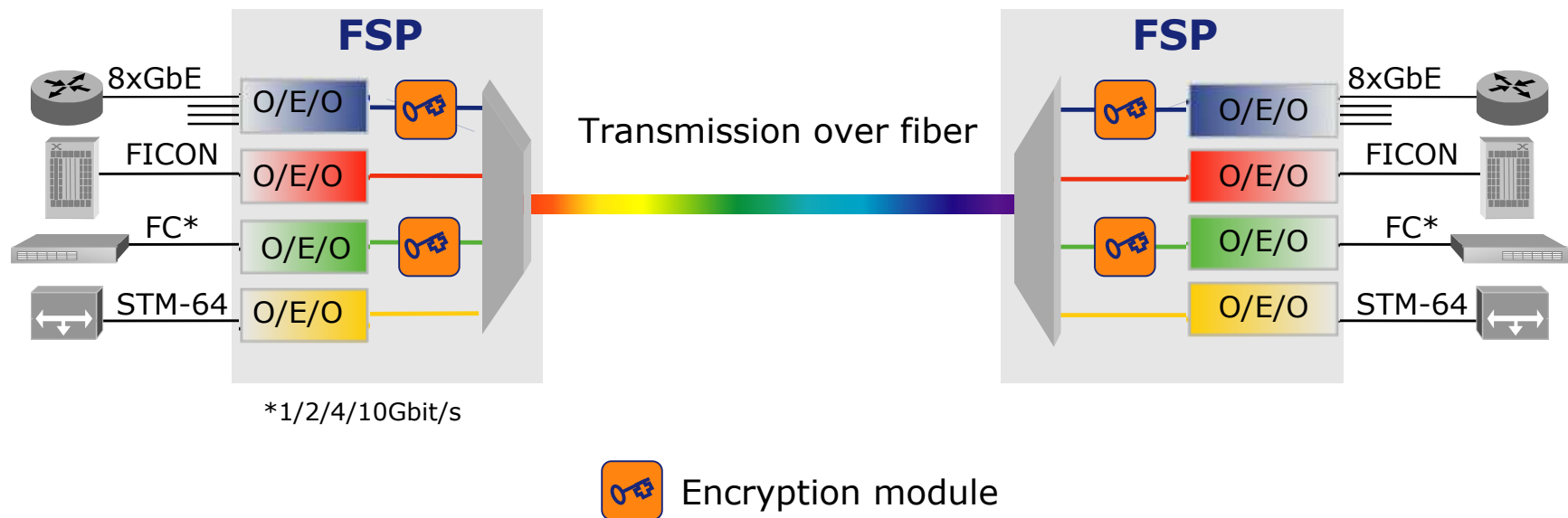


# In-flight encryption of transmitted data

October 2009

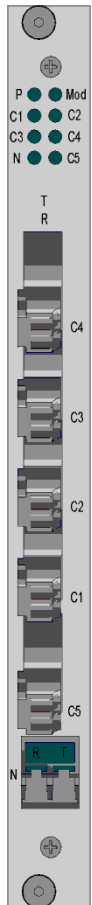
# Transport security

## WDM transmission with encryption



**Modular approach, can be added per channel on an as-needed basis**

# 5TCE - „One card fits all“ concept



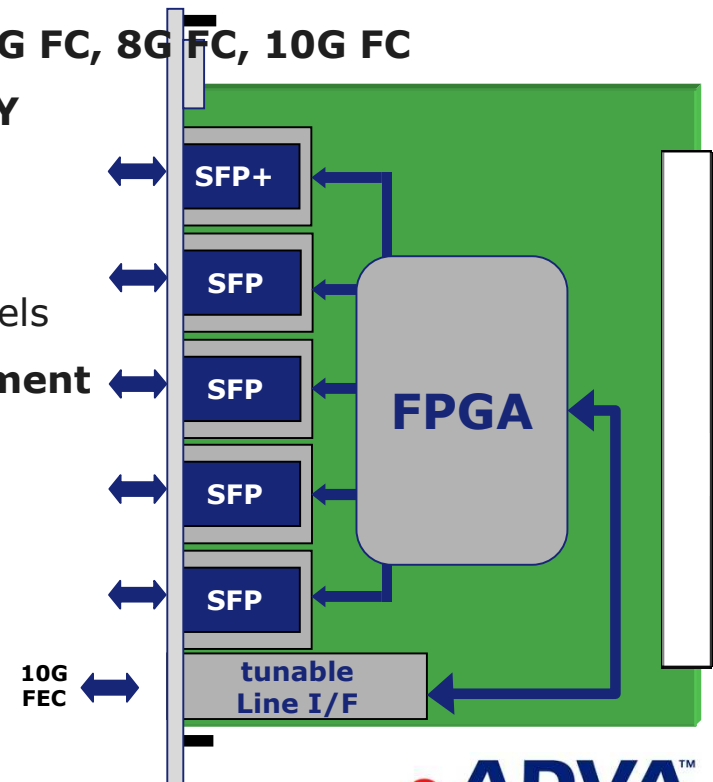
## 5TCE-PCTN-10G

- ▶ **Client ports: 5 x pluggable (SFP/SFP+)**
- ▶ **Network port: 1 x tuneable**
- ▶ **Network Signal: G.709 OTU-2 like incl. S-FEC**
- ▶ **Client applications: 5x 1G/2G FC, 3x 4G FC, 8G FC, 10G FC**

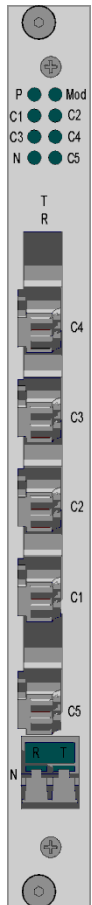
**GbE, 10GE LAN PHY**

**Infiniband**

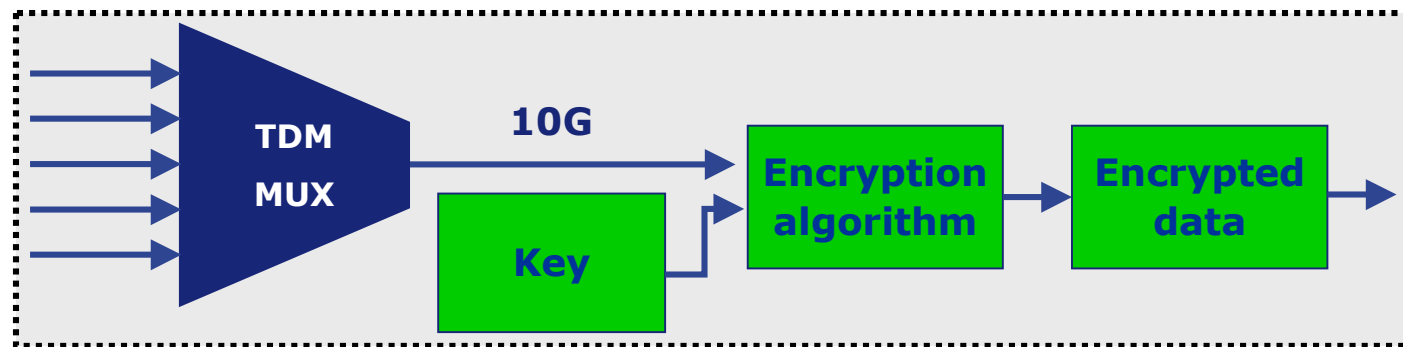
- ▶ **PM: CV, CRC, SE, SES**
- ▶ **Wavelength spectrum: DWDM 80 channels**
- ▶ **Dynamic end-to-end latency measurement**
- ▶ **Constant Bit Rate (CBR) mux mode**
- ▶ **Encryption**



# 5TCE – Encryption Overview



## Data encryption on 5TCE card



- ▶ Encryption applied to the multiplexed data (support of various input signals)
- ▶ AES-256 encryption on the lowest possible layer (low latency)
- ▶ Automatic key exchange (RNG, Diffie-Hellman Algorithm)
- ▶ Addtl. SW load for onboard FPGA
- ▶ Market introduction with R10.1

# Possible Usage Scenarios



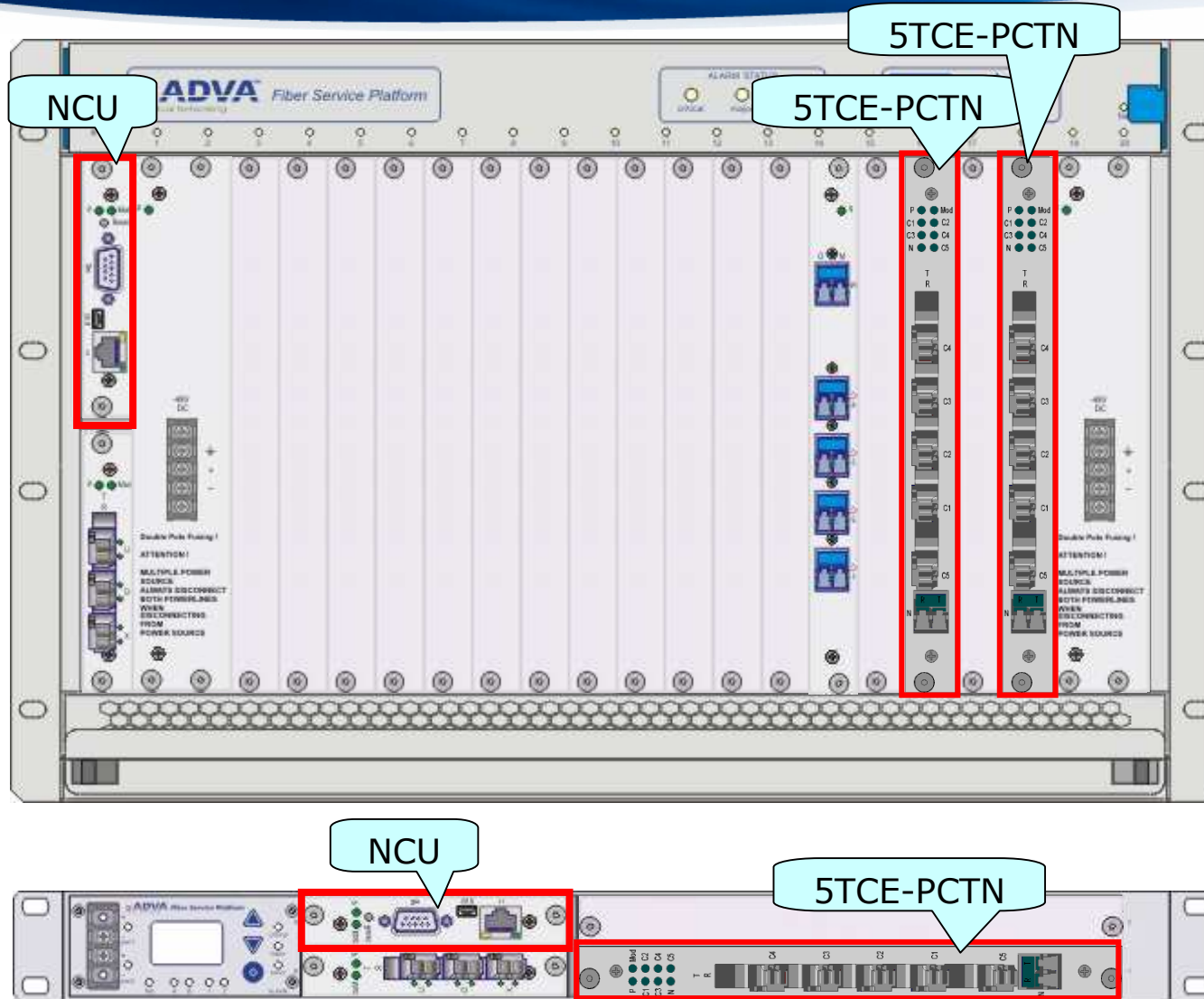
1

## Possible Threat Scenario

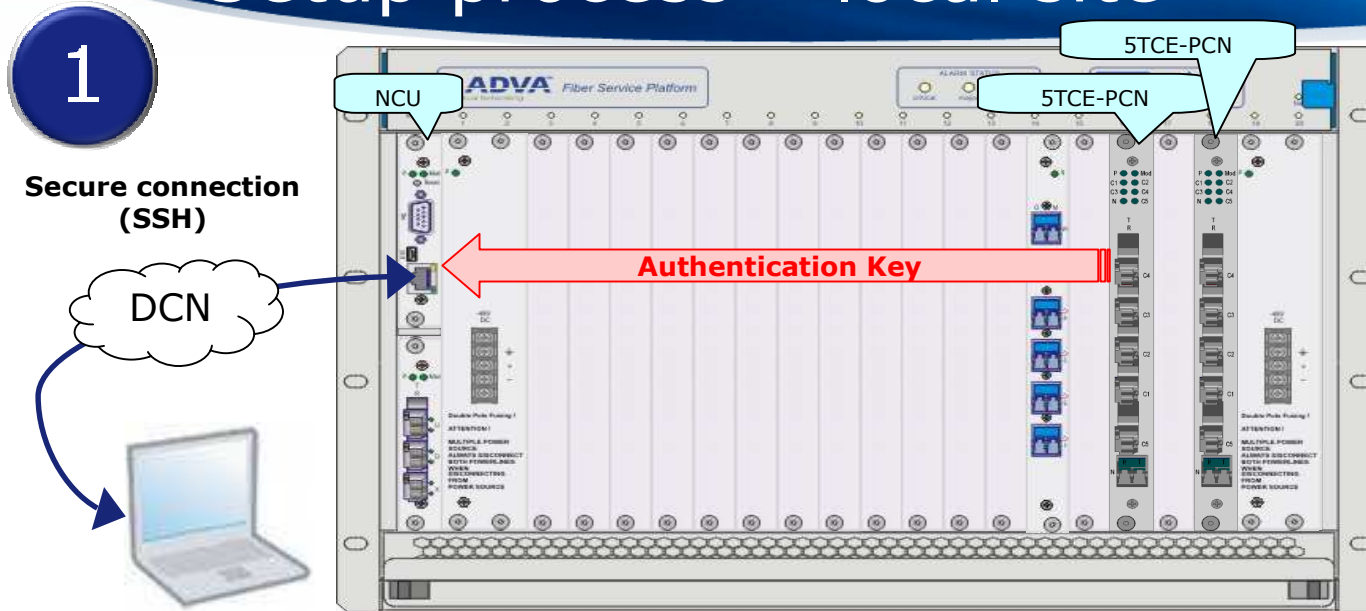
- ▶ intruder is tapping into optical/WDM-link
- ▶ intruder is only listening – no active sending/manipulation of data
- ▶ intruder has no means to intercept communication in order to pretend he is other part of the communication channel

**Authentication via initial password and  
Diffie-Hellman Algorithm offer sufficient protection**

# WDM Encryption Required components

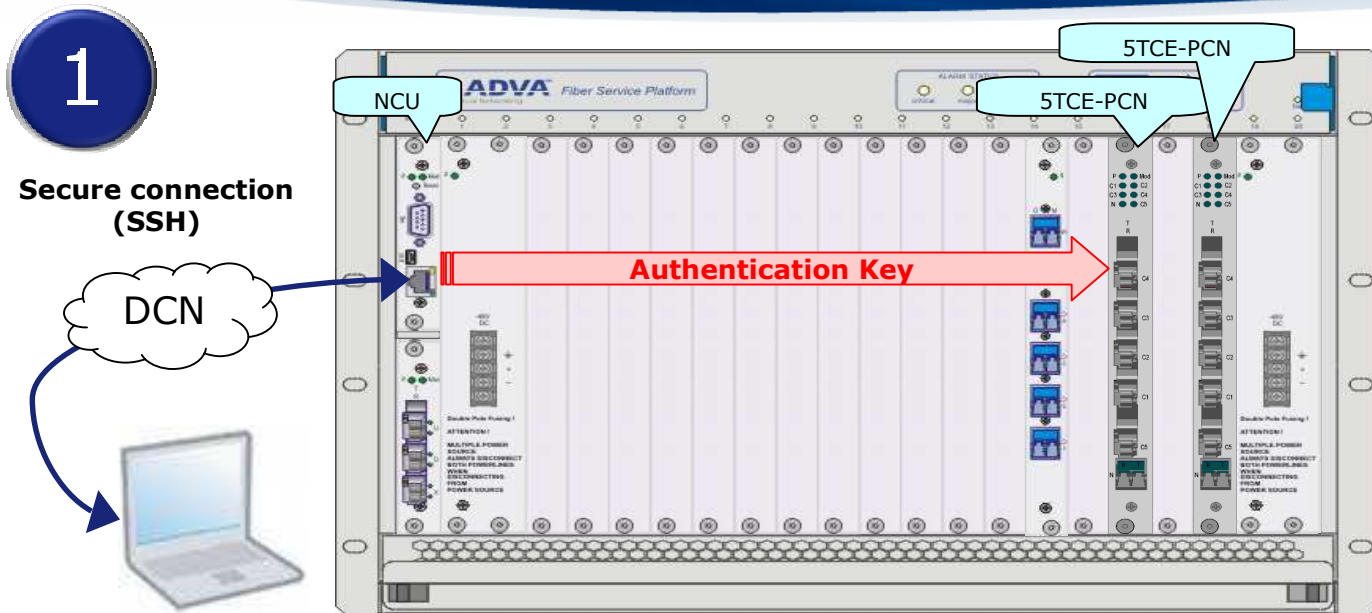


# WDM Encryption Setup process – local site



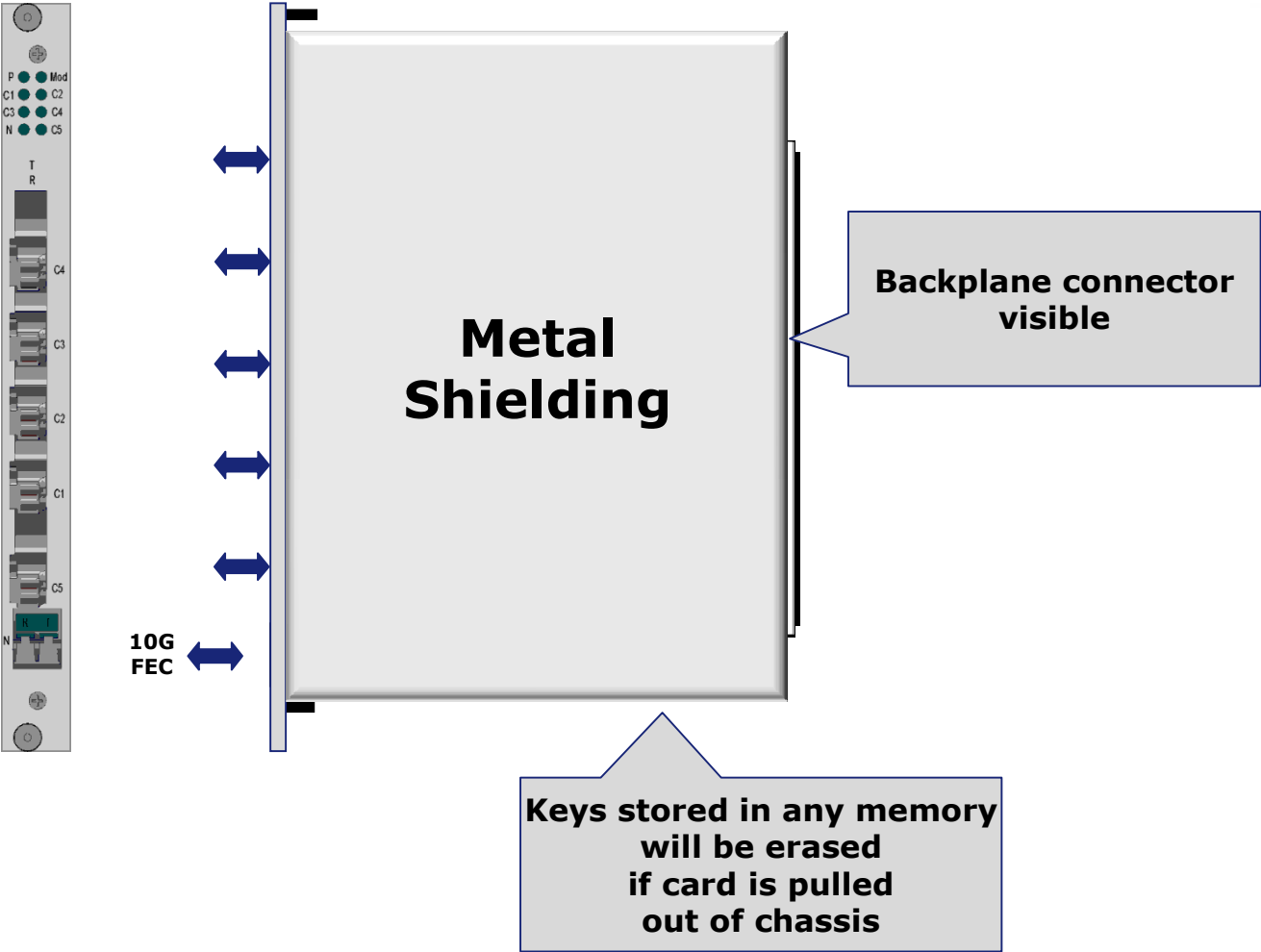
- **Login to Network Control Unit via secure connection (SSH)**
- **Login as "Crypto" ADMIN (no access for other user, at first login Pwd has to be changed)**
- **Authentication key is generated on 5TCE card and stored in NVM on card**
  - **Generated key is stored on Crypto ADMIN Notebook (HDD or USB)**
  - **Stored key is encrypted and protected with Pwd, is valid only for 6 hrs**
  - **Each card in each slot has different Authentication key**
- **After provision of authentication key 5TCE card is trying to start DH process**

# WDM Encryption Setup process – remote site



- Login to Network Control Unit via secure connection (SSH)
- Login as "Crypto" ADMIN (no access for other user, at first login Pwd has to be changed)
- Stored Authentication key is transferred to local 5TCE card
- Authentication key is stored in NVM on local 5TCE card
- After provision of authentication key 5TCE card is trying to establish connection
- After other side responds the DH key exchange process is started
- If valid session key was generated card starts transmitting user data

# HW Implementation



# Detailed implementation

1

Security threat	Tapping of Fiber optic link, no writing of data
Security class	Designed acc. to FIPS 140-2 Level 2
Applied encryption	AES 256, key length 256 bit
Mode of Operation	Counter Mode (CTR) <ul style="list-style-type: none"><li>• Low latency</li><li>• No error propagation</li><li>• Longer re-sync time</li></ul>
Key generation/exchange	Diffie-Hellman, new key 10 minutes <ul style="list-style-type: none"><li>• public key encrypted with authentication key</li></ul>
Initial key setup	Authentication key provided via SSH/DCN, invisible to user
Management	<ul style="list-style-type: none"><li>• All encryption affecting activities only as Crypto ADMIN via SSH/DCN or locally</li><li>• Monitoring as Crypto USER</li><li>• No disabling of encryption</li></ul>
After power down	Session key is lost, continue with DH cycle (using Authent. key)
After link down	Continue with existing session key

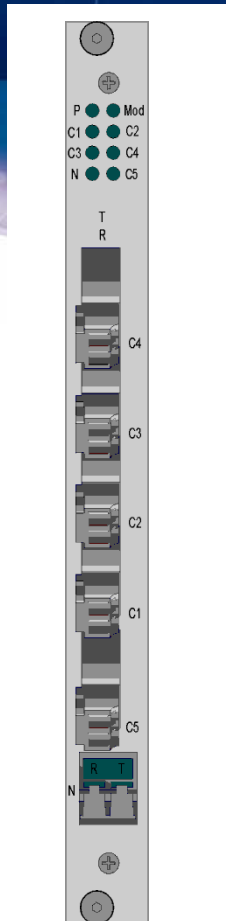
A large, semi-transparent watermark of the ADVA logo is positioned in the background on the right side of the slide. The logo consists of a stylized 'A' made of three curved segments, with a red circle containing a white dot to its left.

ADVANCE

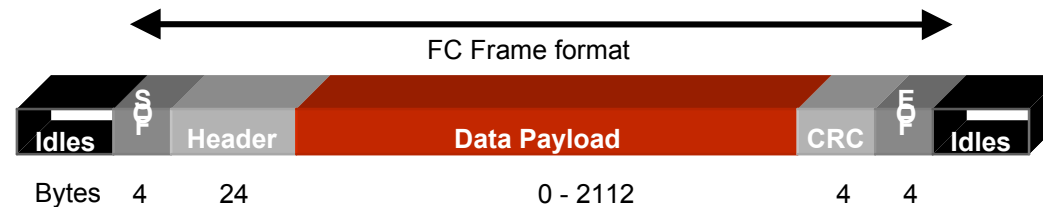
Thank you

[bmoser@advaoptical.com](mailto:bmoser@advaoptical.com)

# 5TCE – Total transparency



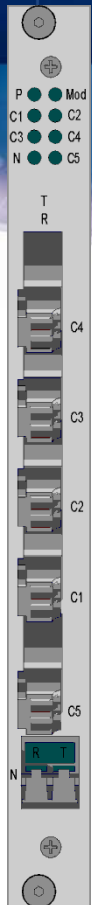
## Constant Bit Rate (CBR) Muxing



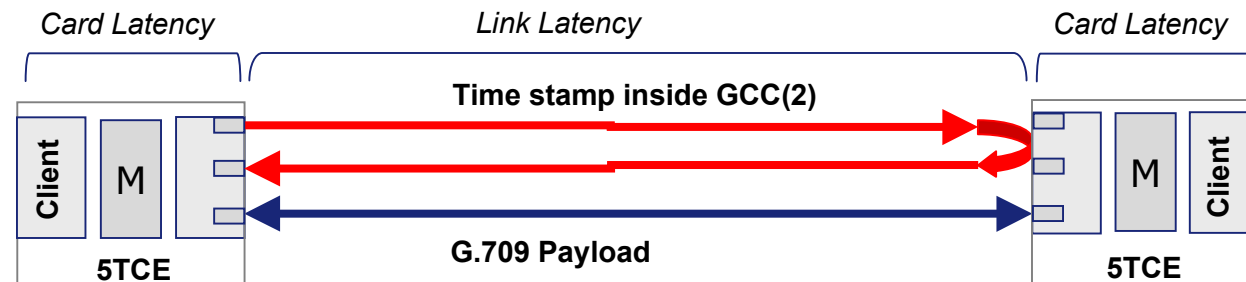
- ▶ Data Integrity is a key requirement for Enterprise Connectivity
- ▶ Today TDM cards are not transparent:
  - ▶ Stuffing inside Idle pattern
  - ▶ Coding layer is stripped before mapping (see also ITU-T G.7041 GFP)
- ▶ Some SAN applications do not "support" TDM in general (ISC-3, VTS, Brocade LD mode, Cisco extended frame size, Cisco PCS signaling...)
- ▶ CBR is a TDM mode that is 100% bit transparent

Standard mode	GE: 2 Slots 1GFC: 1 Slots 2GFC: 2 Slots 4GFC: 4 Slots 8GFC: 8 Slots	CBR mode	GE: 2 Slots 1GFC: 2 Slots 2GFC: 3 Slots 4GFC: 5 Slots 8GFC: 9 Slots
---------------	---	----------	---

# 5TCE – Latency measurement



## Dynamic end-to-end latency measurement

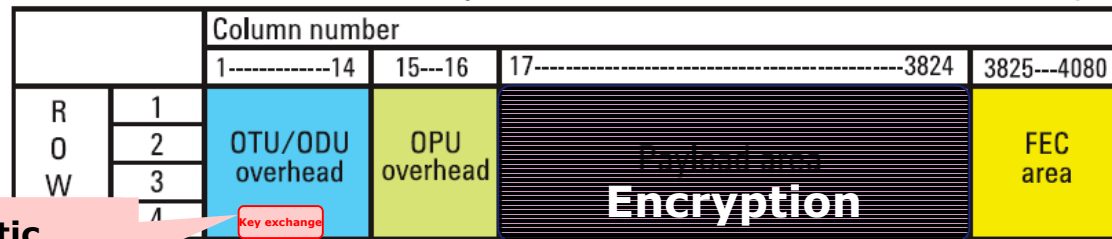
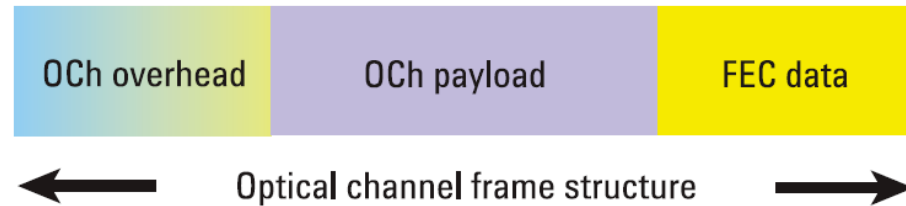


- ▶ Latency is a key criteria for WAN transmission of SAN services
- ▶ Latency is accumulated due to fiber transmission and due to mapping/multiplexing/buffering inside channel cards
- ▶ G.709 – based overhead protocol enabled permanent latency measurement on the link, look-up up table identifies card latency
- ▶ Permanent latency measurement – non-service affecting

# Encryption of 5TCE Remote Link

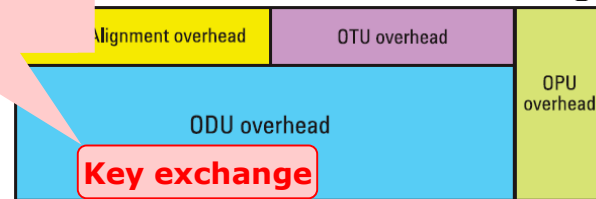
## 5TCE link protocol

- ▶ Data Rate 11.3 Gbps
- ▶ G.709/OTH like framing



Abbreviations	
APS/PCC	Automatic protection switching/ protection communication chann
EXP	Experimental
FAS	Frame alignment signal
FTFL	Fault type and fault location
GCC0-3	General communication channel
JC	Justification control
MFAS	Multi frame alignment signal
NJO	Negative justification opportunity
PM	Path monitoring
PSI	Payload structure identifier
RES	Reserved
SM	Section monitoring
TCM ACT	Tandem connection monitoring activation
TCM1-6	Tandem connection monitoring

Automatic key exchange using DH



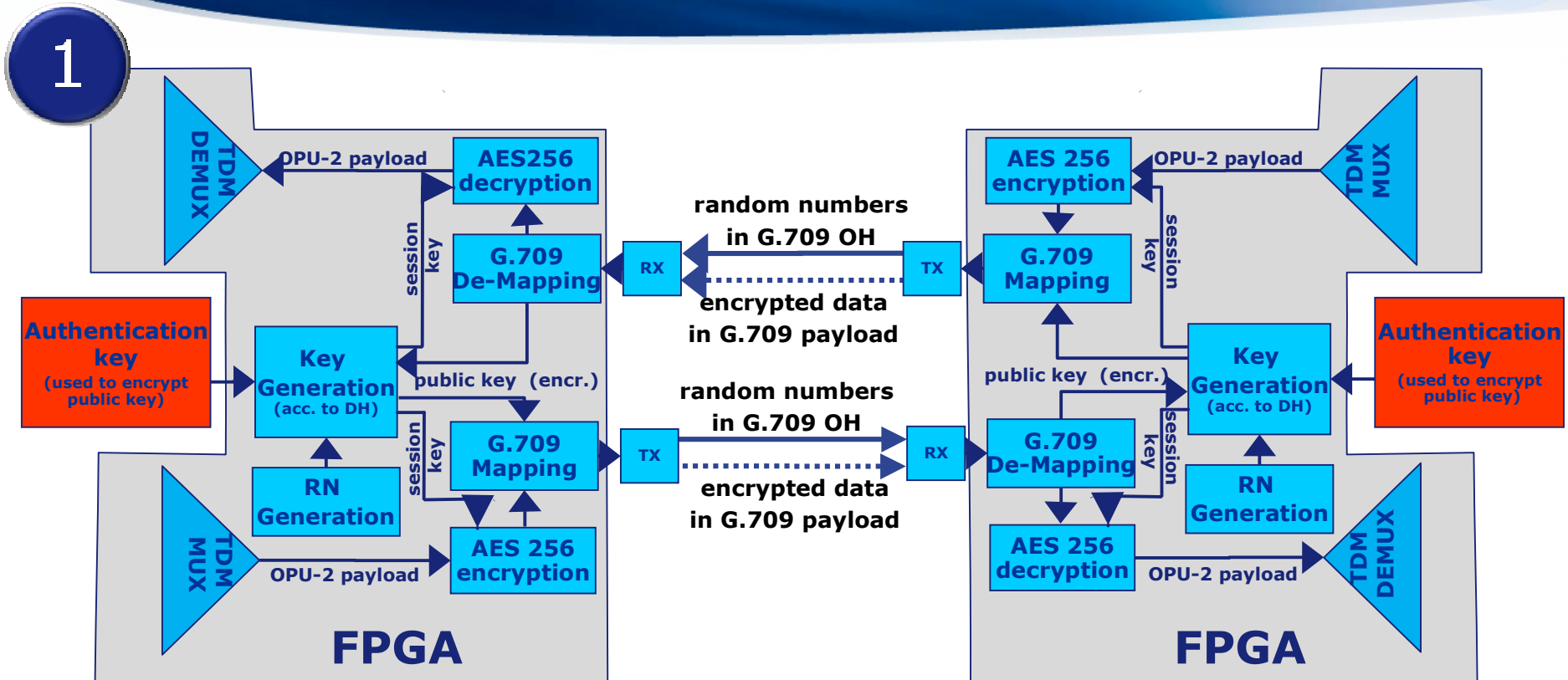
AES256 encrypted OPU2 payload

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	FAS					MFAS	SM			GCC0		RES	RES	JC		
2	RES	TCM ACT	TCM6		TCM5			TCM4		FTFL	RES	JC				
3	TCM3		TCM2		TCM1			PM		EXP	RES	JC				
4	GCC1	GCC2	APS/PCC			RES					PSI	NJO				

# Key procedures

- ▶ General key generation procedure
  - ▶ each side generates its own, secret **private key** (integer)
  - ▶ via DH procedure a **public key** is generated (using the private key)
  - ▶ **public key** is encrypted using the **authentication key** and sent over the link
  - ▶ with the help of **private** and **public key** each side can calculate the **shared secret**
  - ▶ valid **session key** is derived from the **shared secret**
- ▶ All public, private and session keys are erased after usage (exist only in RAM)
- ▶ No encryption relevant keys are stored on NCU
- ▶ Only authentication key is stored in non volatile memory
  - ▶ erased if card is pulled out of chassis

# Implementation Building Blocks



## Key exchange

- ▶ Key-exchange acc. to Diffie-Hellman algorithm (new key every minute)
- ▶ G.709 OH carries integer numbers for session key generation
- ▶ Session key is only kept during usage, erased after application

# Operational limitations

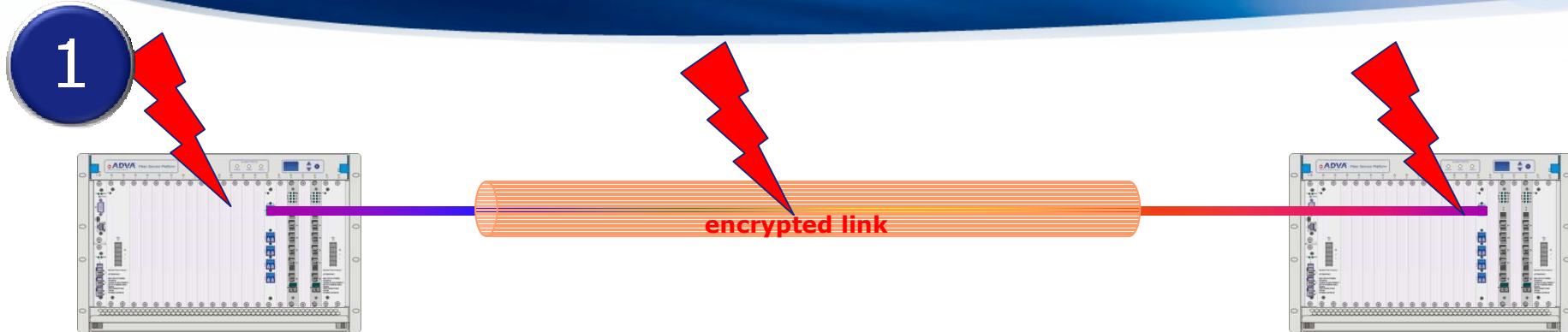
1



## During Operation

- ▶ Local I/Fs only come up after encryption channel is working
  - ▶ First step: configure local and network ports via Ethernet (G.709 link will come up)
  - ▶ Second step: configure/start encryption as Crypto ADMIN (client data will be transmitted)
- ▶ Session key is changed every 10 minutes (via DH algorithm), if key exchange fails operation continues with old session key for max xx min (programmable)
- ▶ Monitoring/management
  - ▶ Encryption settings can only be done via Crypto ADMIN role
  - ▶ Crypto USER can only read the relevant encryption parameters
  - ▶ Encryption related activities will trigger an event-trap
  - ▶ Specific destination for Crypto TRAPS can be defined
- ▶ Encryption cannot be turned off or stopped
  - ▶ Test mode for 30mins, can only be engaged by Crypto ADMIN
- ▶ 2 different 5TCE-versions: 5TCE with encryption can only operate with encryption ON
- ▶ Only the whole payload (=all user interfaces can be encrypted)
- ▶ LED indicates running encryption

# Operational limitations



## After Power Down

- ▶ Session key is lost, start new DH cycle with stored Authentication key

## After Link down /Link loss

- ▶ Session key is stored, continue with current session key

# Crypto specific settings

- ▶ Crypto ADMIN settings
  - ▶ Change own password and password of Crypto USER (**mandatory at first login**)
  - ▶ Initiate Authentication Key generation (local and remote)
  - ▶ Define lifetime of session key: 30min, 60min, never expires
  - ▶ Define destination of Crypto TRAPS
  - ▶ Define severity of Crypto TRAPS
  - ▶ Engage test modus (expires after 30 mins)
  - ▶ Enable/disable local USB/serial ports
  
- ▶ Crypto monitoring parameters
  - ▶ Successful/unsuccessful key exchanges
  - ▶ Encryption up-time
  - ▶ Time until next key exchange
  - ▶ Unsuccessful logins as Crypto ADMIN