

# Състояние на QKD стандартизацията

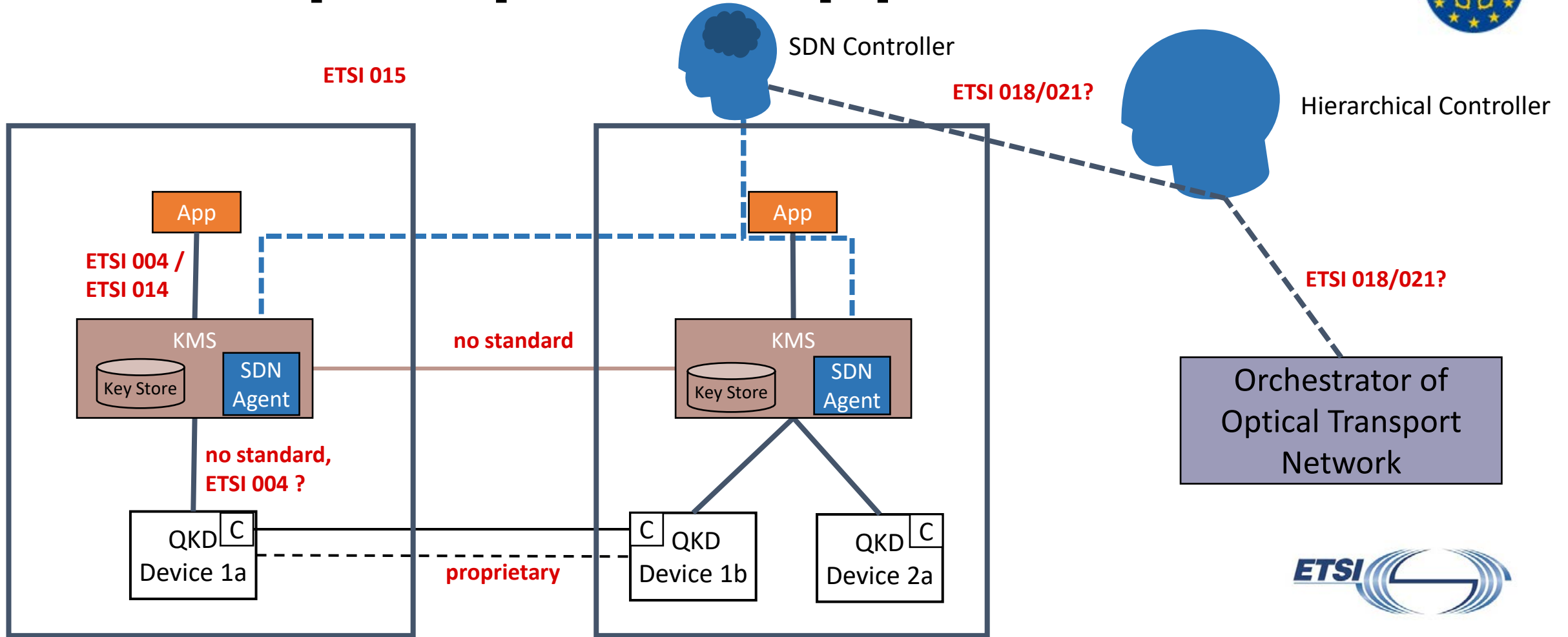
- Стандартите са важни
- Работата по QKD стандартите едва е започнала
- Различни стандартизиращи организации изработват стандарти, съобразявайки се само частично едни с други
- Различни подходи при ETSI и ITU-T: отдолу-нагоре и отгоре-надолу
- Първите версии на най-важните стандарти са публикувани
- Много празнини трябва да бъдат попълнени

[www.euroqci.bg](http://www.euroqci.bg)

*Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.  
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.  
Нито Европейският съюз, нито съфинансиращият орган не носят отговорност за тях.*



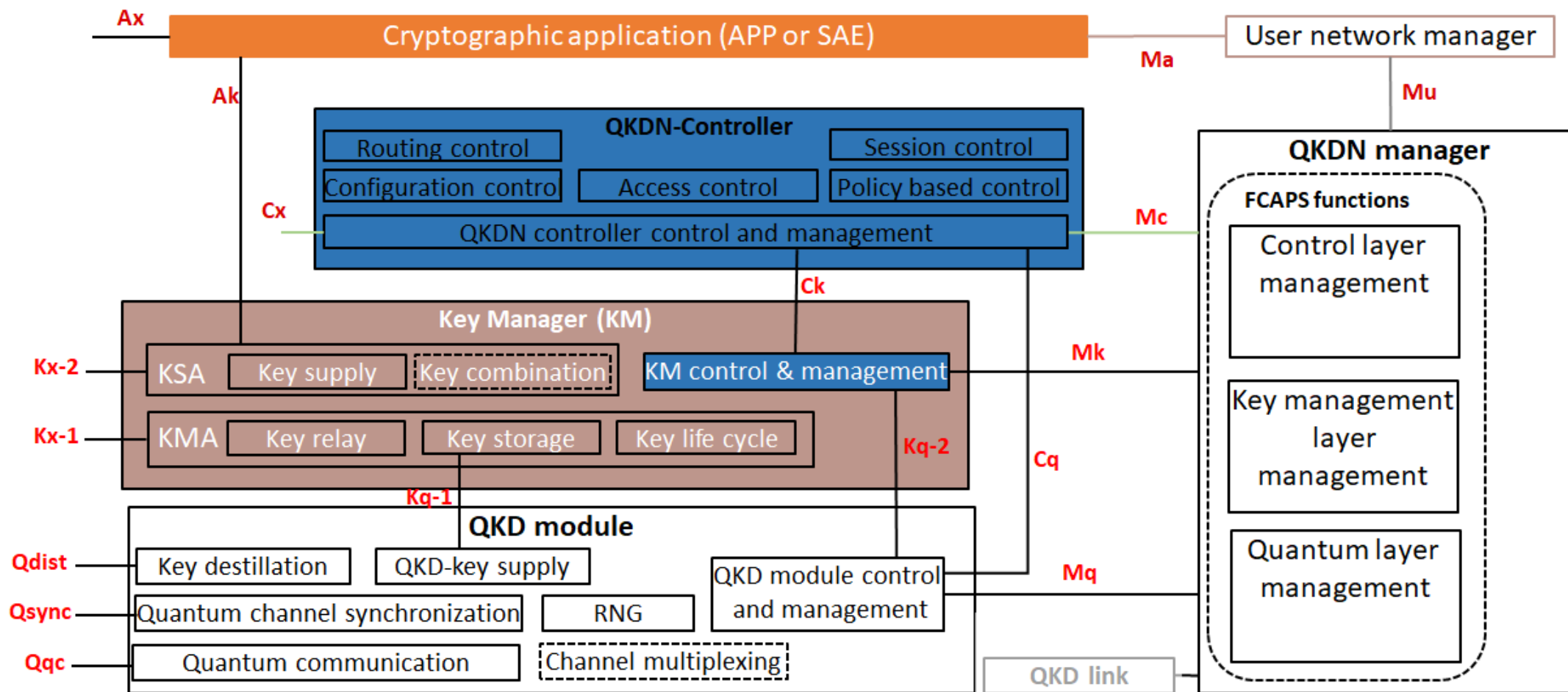
# Стандартизирани интерфейси



[www.euroqci.bg](http://www.euroqci.bg)



# ITU-T Y.3802 интерфейси





# ITU-T Study Group 13 **ПОДХОД ОТГОРЕ НАДОЛУ**

## Published documents

- Y.3800: Overview on networks supporting QKD
- Y.3801: Functional Requirements of QKDN
- Y.3802: Functional Architecture of QKDN
- Y.3803: Key Management for QKDN
- Y.3804: QKDN – Control and Management
- Y.3805: QKDN – SDN Control
- Y.3806: QKDN – Requirements for QoS Assurance
- Y.3807: QKDN – QoS Parameters
- Y.3808: Integration of QKDN and Secure Storage Networks
- Y.3809: Business Role Models for QKDN
- Y.3810: QKDN Interworking Framework
- Y.3811: Functional Architecture for QoS Assurance for QKDN
- Y.3812: Requirements of ML-based QoS Assurance for QKDN
- Y.3813: QKDN Interworking – Functional Requirements
- Y.3814: QKDN – Functional Requirements and Architecture for ML Enablement

## Unpublished work items

- Y.3815 “QKDN – overview of resilience”
- Y.3816 “QKDN – Functional architecture of ML based QoS assurance”
- Y.3817 “QKDN – Requirements of QoS assurance”
- Y.3818 “QKDN interworking – architecture”
- ITU-T Y.QKDN-fr “Framework for QKDN Federation”
- ITU-T Y.QKDNi-SDNC “QKDN Interworking – SDN Control”
- ITU-T Y.Supp.QKDN-UC “Uses Cases of QKDNs”
- ITU-T Y.QKDN-rsrq “Requirements for quantum key distribution network resilience
- ITU-T Y.QKDN-amc “QKDN – Requirements and architectural model for autonomic management and control
- ITU-T Y.QKDN-TSNfr “Framework for integration of QKDN and time sensitive network
- ITU-T Y.QKDN\_SSNarch “Functional architecture for integration of QKDN and secure storage network”
- ITU-T Y.QKDN\_SSNreq “Functional requirements for integration of QKDN and secure storage network”
- ITU-T Y.QKDN-qos-auto-rq “QKDN – Requirements for autonomic QoS assurance
- ITU-T Y.QKDN-qos-mmq “QKDN – Measurement methodology for QoS parameters”



# ETSI ISG QKD: подход отдолу нагоре

## Published work items

- GS QKD 002: QKD Use Cases
- GR QKD 003: Components and Internal Interfaces
- GS QKD 004: Application Interface
- GS QKD 005: QKD Security Proofs
- GR QKD 007: Vocabulary
- GS QKD 008: QKD Module Security Specification
- GS QKD 011: Component Characterization
- GS QKD 012: Device and Channel Parameters for QKD Deployment
- GS QKD 014: Protocol and Data Format of REST-based Key Delivery API
- GS QKD 015: Control Interface for SDN
- GS QKD 016: CC Protection Profile – Pair of Prepare and Measure QKD modules
- GS QKD 018: Orchestration Interface for SDN

## Unpublished work items

- GS QKD 013: Characterization of Optical Output of QKD transmitter modules
- GR QKD 017: Network Architectures
- GR QKD 019: QKD Design of QKD interfaces with authentication
- GS QKD 020: QKD Protocol and Data Format of REST-based Interoperable KMS API
- GS QKD 021: QKD Orchestration Interface for Software Defined Networks



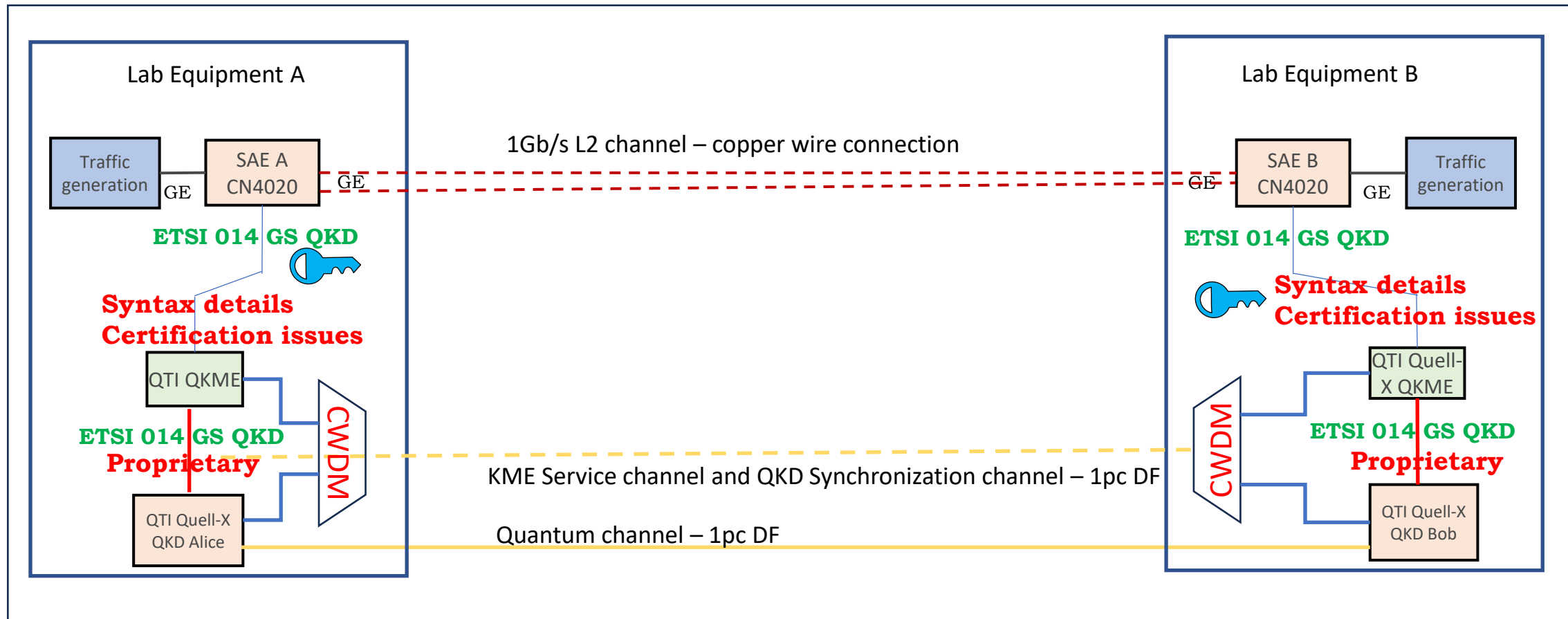
[www.euroqci.bg](http://www.euroqci.bg)

*Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.*

*Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.*

*Нито Европейският съюз, нито съфинансиращият орган не носят отговорност за тях.*

# Практически проблеми на взаимодействието



# Практически проблеми на взаимодействието

- Липса на стандарти
- Използване на частни протоколи
- Умишлено или случайно въздействие върху детайли на стандарта (синтаксис)
- Разлики в изискванията за сигурност и сертифициране
- Използване на несъвместими версии на протоколи (TLS)

SDH GPT STM-1 mapping

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63

SDH Alcatel STM-1 mapping

1	10	19	4	13	22	7	16	25
2	11	20	5	14	23	8	17	26
3	12	21	6	15	24	9	18	27
28	37	46	31	40	49	34	43	52
29	38	47	32	41	50	35	44	53
30	39	48	33	42	51	36	45	54
55	58	61	56	59	62	57	60	63

Resulting interconnection

1	-	-	4	-	-	7	-	-
-	11	-	-	14	-	-	17	-
-	-	21	-	-	24	-	-	27
28	-	-	31	-	-	34	-	-
-	38	-	-	41	-	-	44	-
-	-	48	-	-	51	-	-	54
55	-	-	-	59	-	-	-	63

No.	Method name	URL	Access Method
1	Get status	https://{KME_hostname}/api/v1/keys/{slave_SAE_ID}/status	GET
2	Get key	https://{KME_hostname}/api/v1/keys/{slave_SAE_ID}/enc_keys	POST (or GET)
3	Get key with key IDs	https://{KME_hostname}/api/v1/keys/{master_SAE_ID}/dec_keys	POST (or GET)