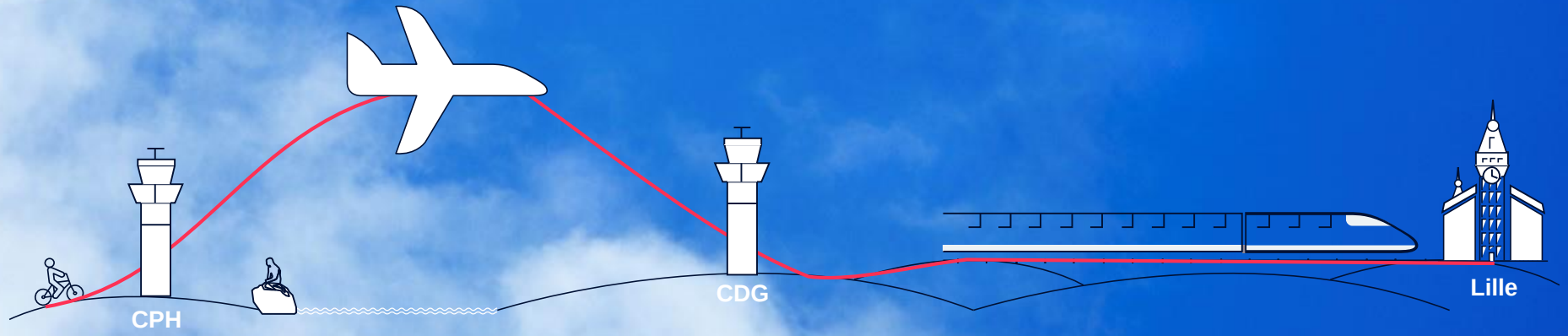
Optical Encryption

First line of defense for Network Services

FT02 | Tuesday 14:35 - 14:55 | FIC
Talk | kristian.andersson@nokia.com

Secure Transport

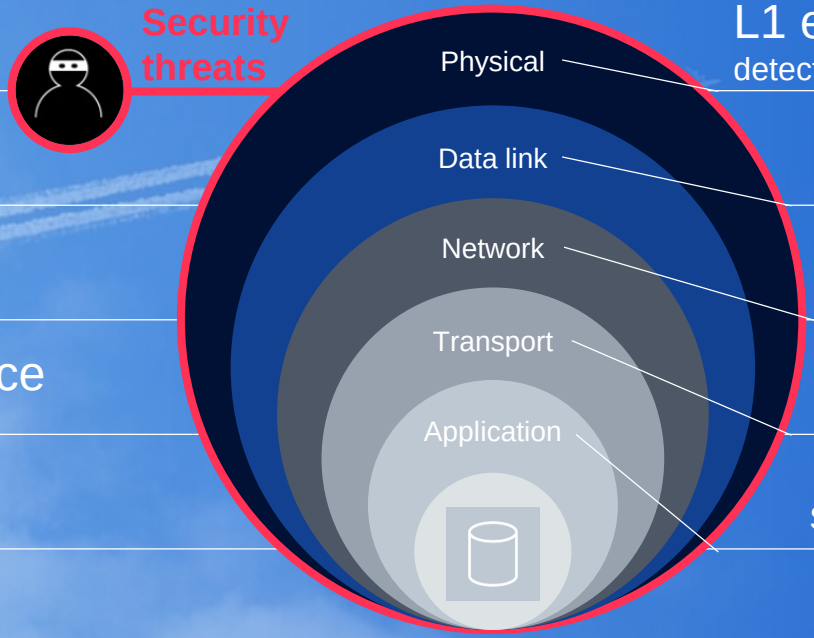
replacing Illusions by Trust



NOKIA

Why Optical Encryption?
First line of defense for Network Services

- Reduced cost
- Low latency
- Transparency
- Better performance
- High availability
- Management



L1 encryption, monitoring, Intrusion detection, optical span protection

MacSec encryption

IPSec encryption

TCP, UDP privacy and data integrity protocols

SSL/TLS encryption

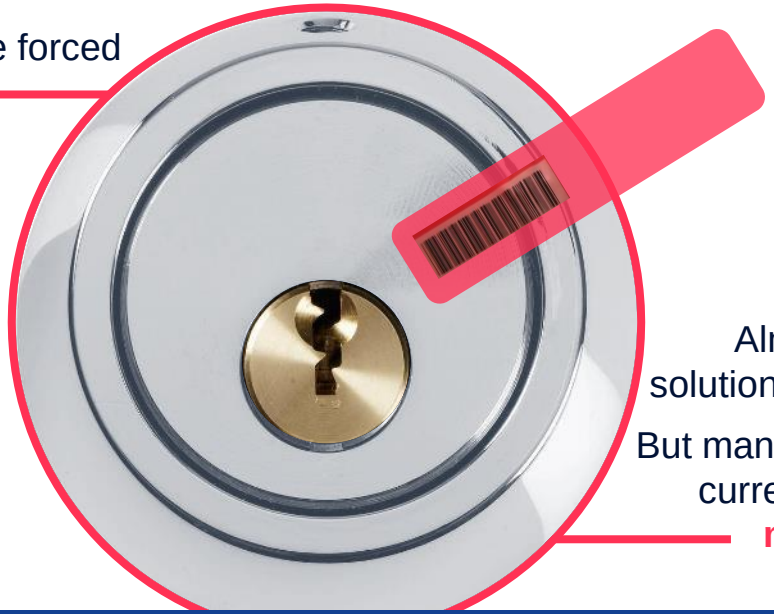
NOKIA

Illusion of Security

Home Security

Every home has looks on doors.

But 90+% house locks can be forced in **less than 15 seconds** without any evidence of unauthorized entry.



Network Security

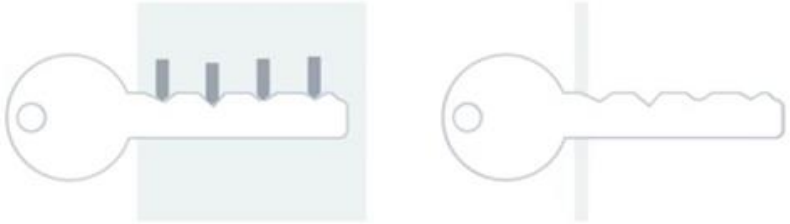
Almost all optical transport solutions claim they are secure.

But many solutions **do not meet** current recommendations on **minimum key strength.**

Well-balanced cryptographic solutions with a Tamper-Resistant lock and Quality Key

Let’s begin with the key Aspect – the Key Strength

Algorithm	Effective security strength	Security under quantum attack
Asymmetric RSA-2048	112 bit key strength	Hackable “Lack of Trust”
Symmetric AES-256	256 bit key strength	Quantum-proof: over 1,000,000 years to successful quantum computer attack*



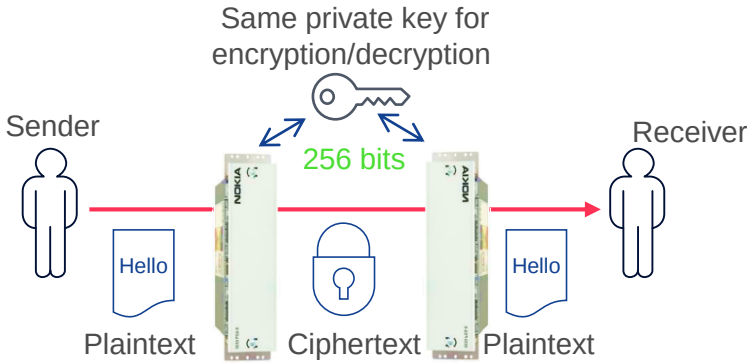
* Exceeds NSA recommendations for classified data

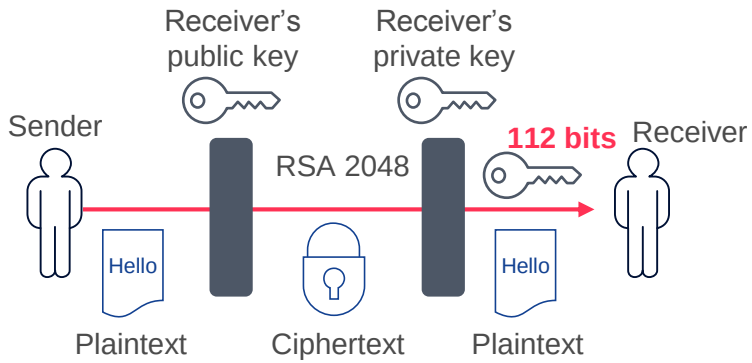
* using quality key refreshed every hour

NOKIA

Comparing Key Strengths

based on Symmetric vs. Asymmetric Algorithms



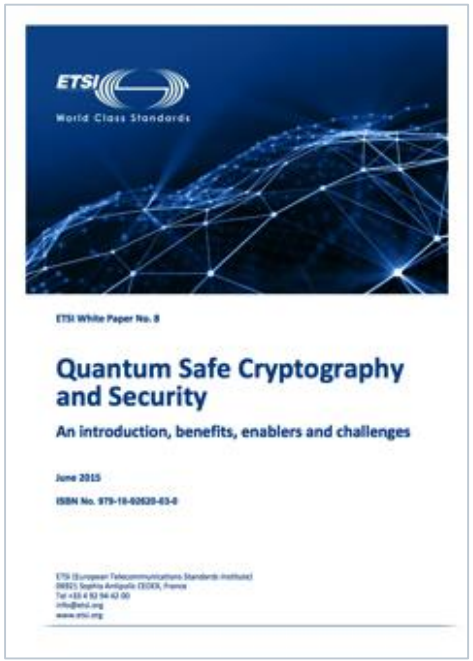


SYMMETRIC	CRITERIA	ASYMMETRIC
Secure private	Key type	Public and private
Low	CPU power needed	High
True random key	Entropy	Integer factorization

NOKIA

Cryptographically comprehensive solutions ensure Key Quality for the Future

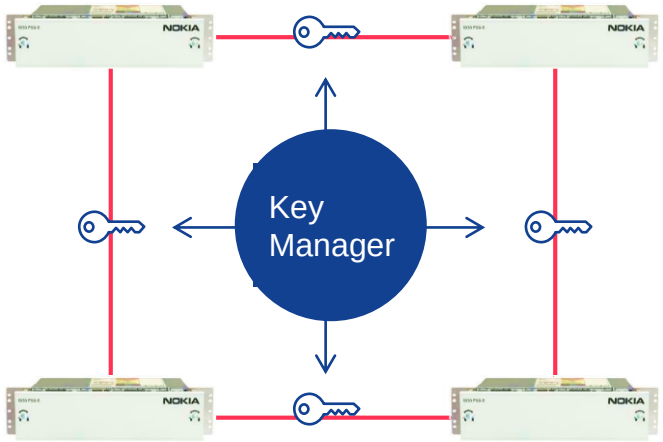
Must balance Cipher and Key Strength

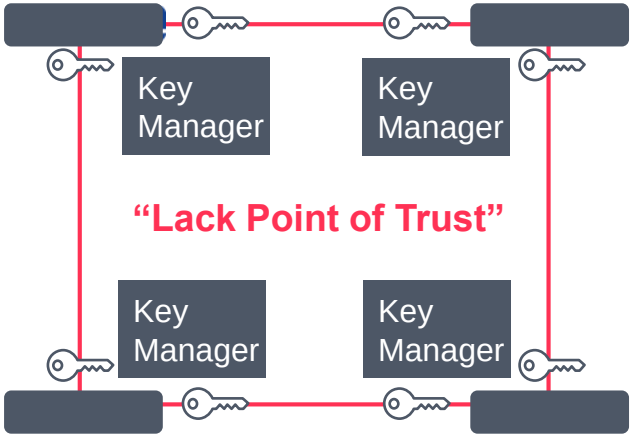


Comparison of conventional and quantum security levels of some popular ciphers

Algorithm	Key length	Effective key strength/security level	
		Conventional computing	Quantum computing
RSA-1024	1013 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

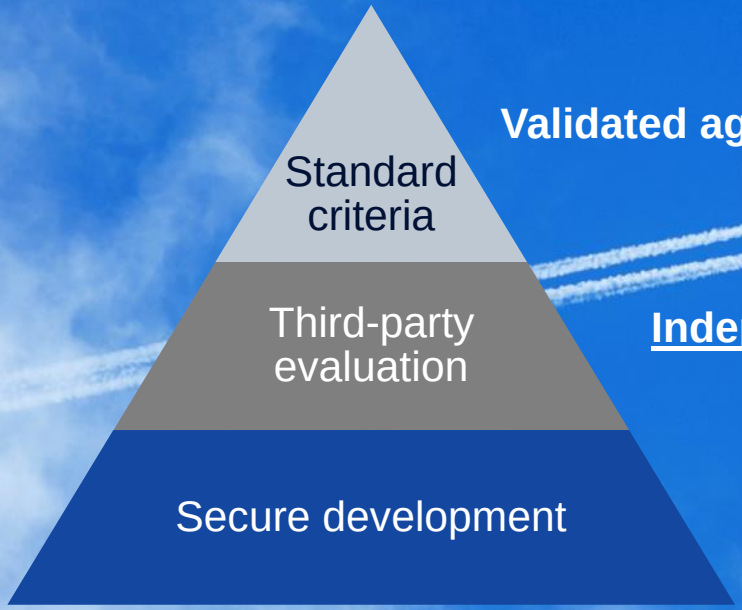
Another linked aspect to compare is Key Management





CENTRALIZED	CRITERIA	DISTRIBUTED
Single	Points of trust	Multiple
Consistent	Policy enforcement	Inconsistent
Unified	Key revocation	Uncoordinated
Good	Scalability	Poor

Insist on Independently Certified solutions – *“replacing Illusions by Trust”*



Validated against open security standards

<u>Independent</u> certification is proof of due diligence

Developed in accordance with a rigorous manufacturing process

Common Criteria

ANSSI Agence nationale de la sécurité des systèmes d'information

NIST National Institute of Standards and Technology U.S. Department of Commerce

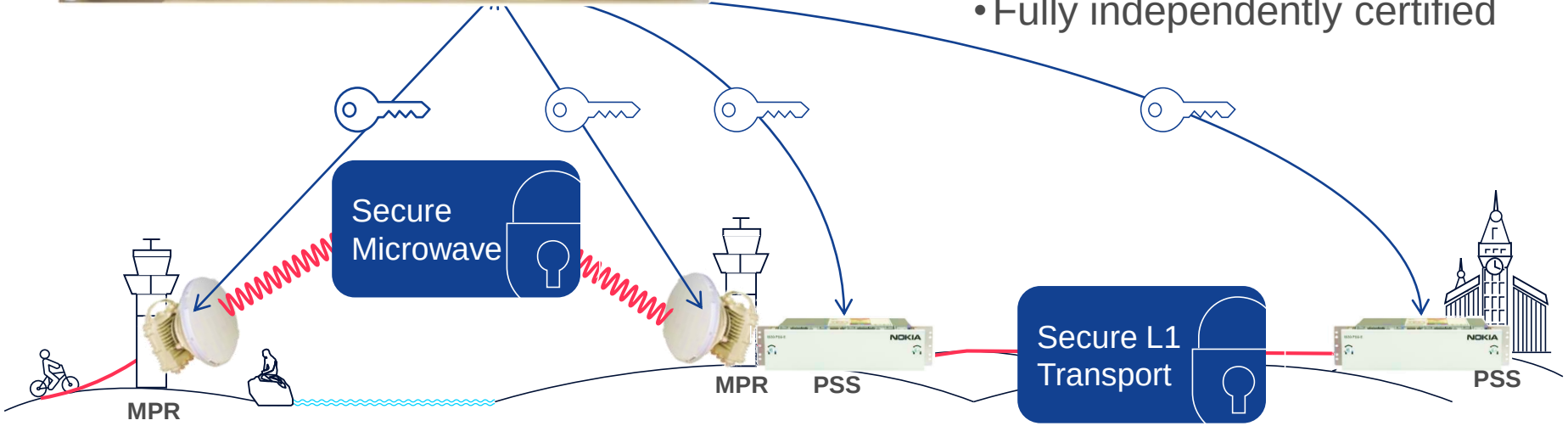
FIPS 197 AES Encryption Approved

NOKIA

Turn to Nokia for Comprehensive Quantum-Safe Certified Encryption and Trust your First line of defense for Network Services

- Effective Layer 1 encryption
- Optical intrusion detection
- Centralized, unified key mgmt.
- Fully independently certified

Nokia 1830 Security Management Server



Secure Nokia Transport

replacing Illusions by Trust

Optical transport layer security including Quantum-Safe L1 encryption provides a first line of defense complementing security strategies at other layers

Simple, unified and centralized key management required: ensure solutions are Certified and independently validated

Solutions are available today, “but seeing is believing”
Welcome to our Demo at B20

NOKIA


NOKIA

Copyright and confidentiality