

Optical Encryption

NOKIA

The Nokia logo is rendered in a light blue, semi-transparent font. A white streak, resembling a jet contrail, cuts across the logo from the bottom left to the top right, passing through the letters 'O', 'I', and 'K'.

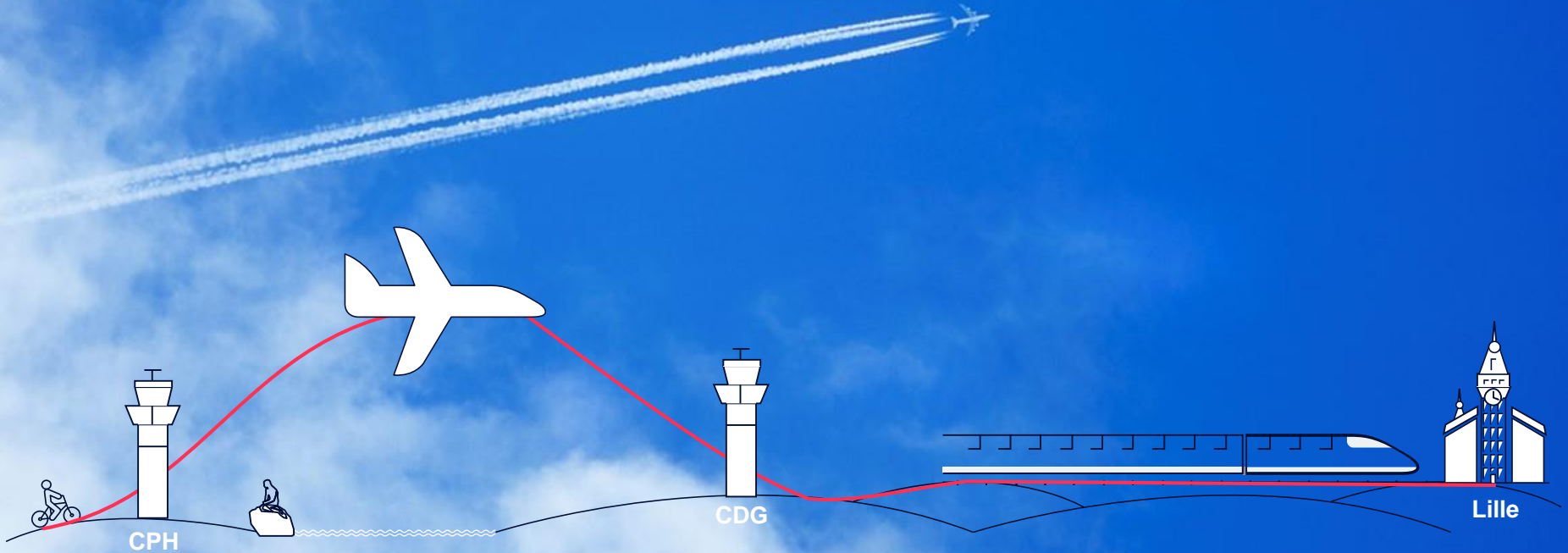
First line of defense for Network Services

Confidential

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

Secure Transport

replacing Illusions by Trust

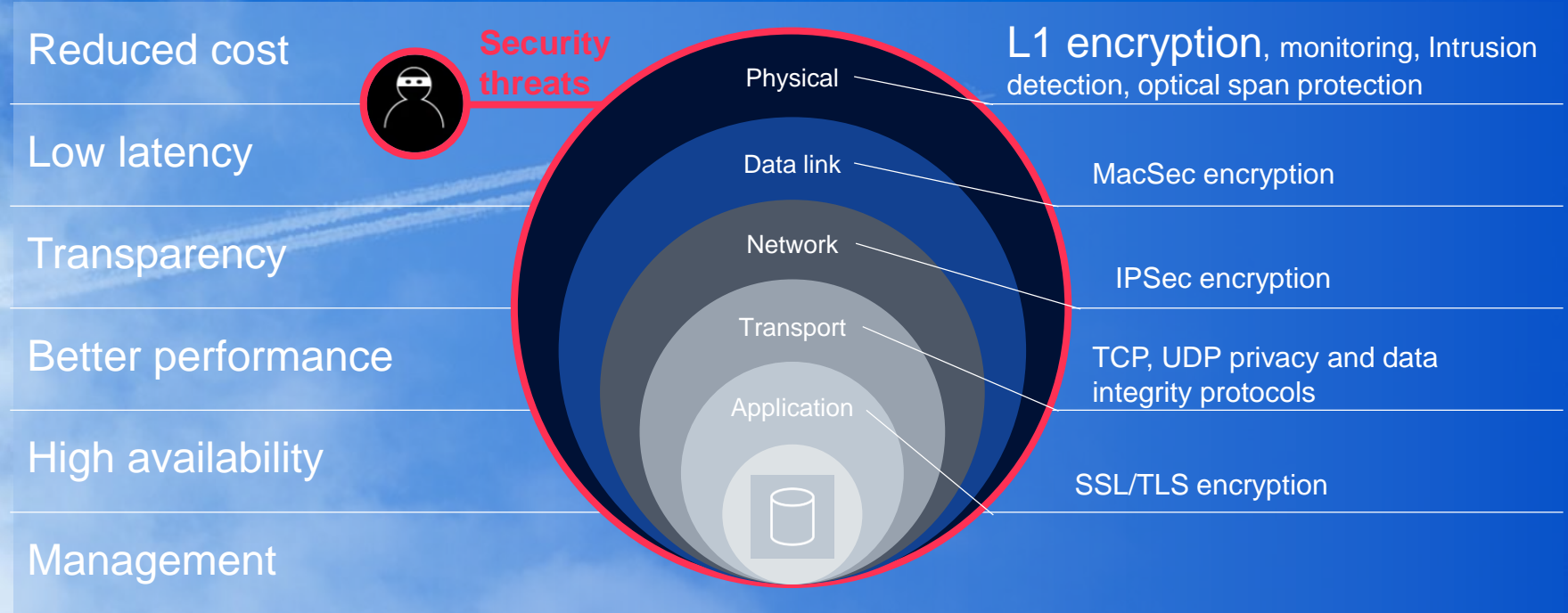


Confidential

NOKIA

Why Optical Encryption?

First line of defense for Network Services

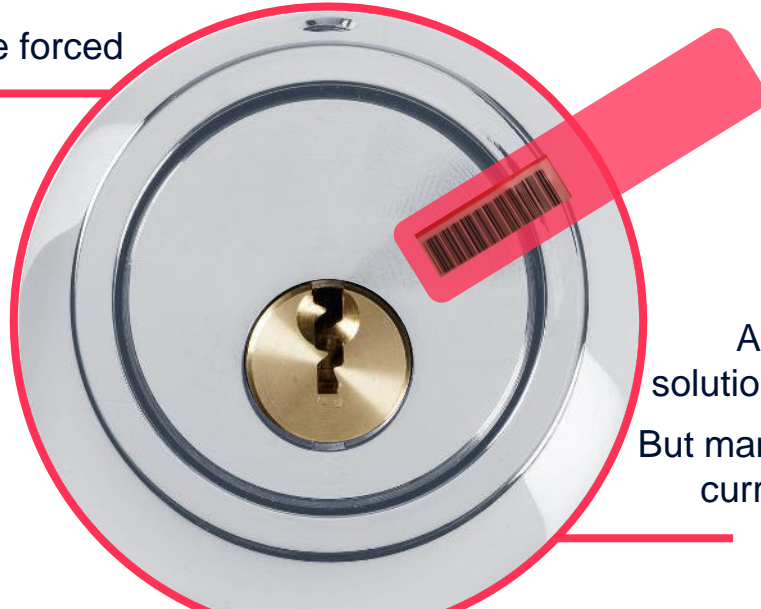


Illusion of Security

Home Security

Every home has locks 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

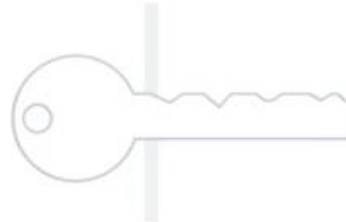
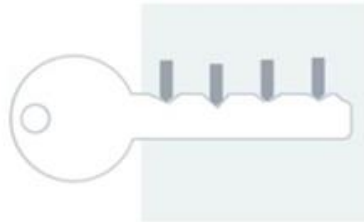
Let's begin with the key Aspect – the Key Strength

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

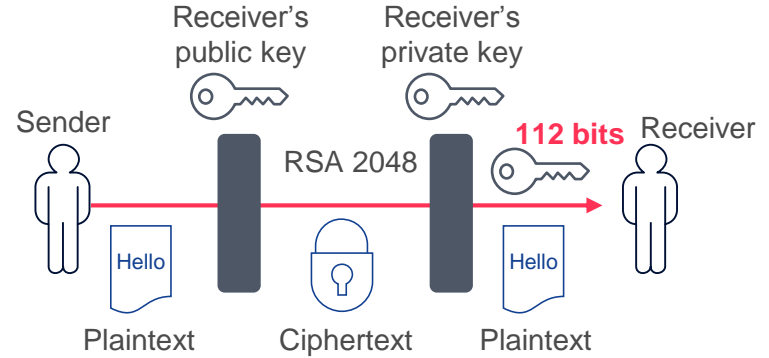
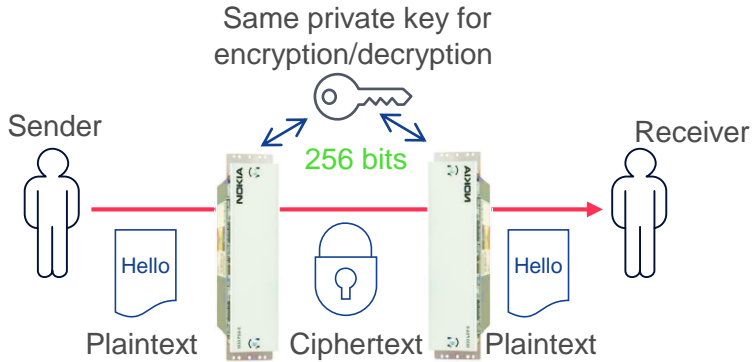
over 1,000,000 years to successful quantum computer attack*

* Exceeds NSA recommendations for classified data

* using quality key refreshed every hour

Comparing Key Strengths

based on Symmetric vs. Asymmetric Algorithms



SYMMETRIC

Secure private

Low

True random key



CRITERIA

Key type

CPU power needed

Entropy



ASYMMETRIC

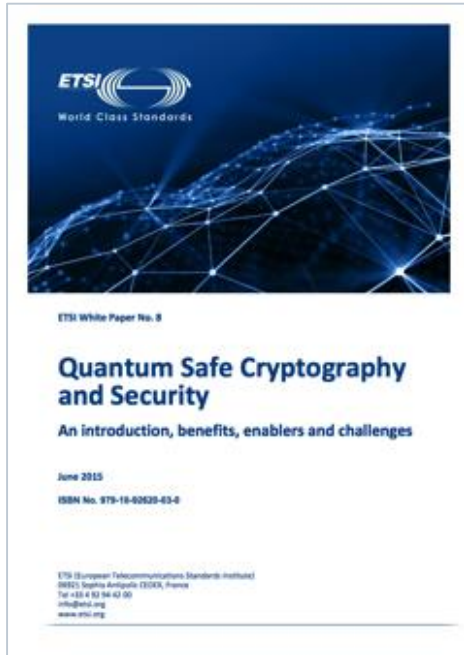
Public and private

High

Integer factorization

Cryptographically comprehensive solutions ensure Key Quality for the Future

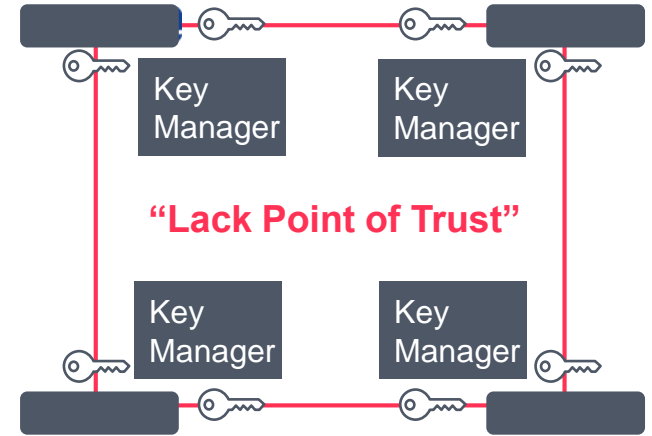
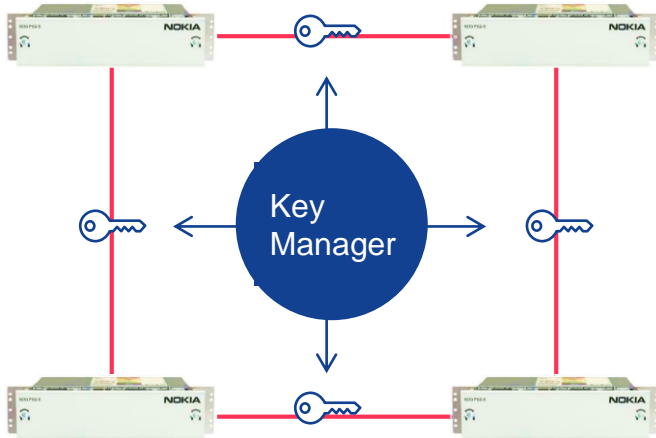
Must balance Cipher and Key Strength



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	Yellow	0 bits	Red
RSA-2048	2048 bits	112 bits	Green	0 bits	Red
ECC-256	256 bits	128 bits	Green	0 bits	Red
ECC-384	384 bits	256 bits	Green	0 bits	Red
AES-128	128 bits	128 bits	Green	64 bits	Yellow
AES-256	256 bits	256 bits	Green	128 bits	Green

Another linked aspect to compare is Key Management



CENTRALIZED

Single
Consistent
Unified
Good



CRITERIA

Points of trust
Policy enforcement
Key revocation
Scalability

DISTRIBUTED

Multiple
Inconsistent
Uncoordinated
Poor



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



ANSSI



Agence nationale
de la sécurité
des systèmes d'information

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

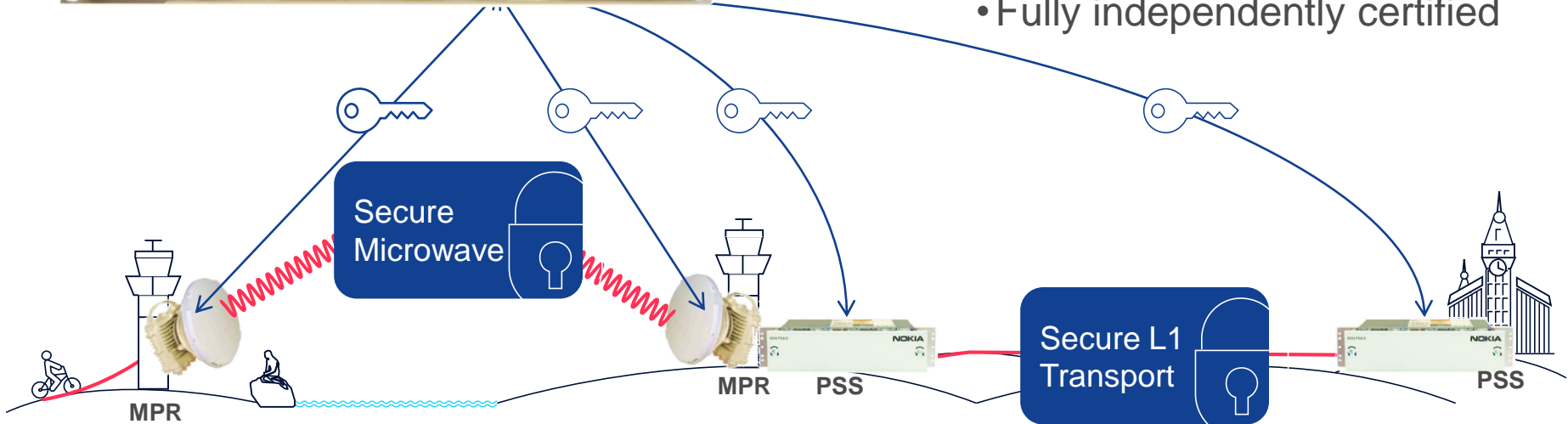


Turn to Nokia for Comprehensive Quantum-Safe Certified Encryption and Trust your First line of defense for Network Services

Nokia 1830 Security Management Server



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



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

The image features the word "NOKIA" in a large, bold, light blue sans-serif font, centered horizontally. The background is a vibrant blue sky filled with soft, white, wispy clouds. A white contrail from an airplane streaks diagonally across the sky, passing behind the letters of "NOKIA". The overall composition is clean and modern, evoking a sense of global connectivity and technology.

NOKIA

Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use of Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback"). Such Feedback

may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular

purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.