



# TESTING AND EVALUATION INFRASTRUCTURE FOR THE EUROPEAN QUANTUM COMMUNICATION INFRASTRUCTURE (EUROQCI) INITIATIVE

TOPIC ID: CNECT/2023/OP/0032

ETSI/ IQC Quantum Safe Cryptography Conference, Singapore, May 16<sup>th</sup> 2024  
Martin Stierle

## NOSTRADAMUS PROJECT PRESENTATION

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.



# Introduction and General Overview

# NOSTRADAMUS OBJECTIVE



## Blueprint for a Testing & Validation Infrastructure

*“It is the goal of this Consortium to describe the blueprint for a Testing & Validation Infrastructure in order to enable the evaluation and certification of QKD devices and related technologies, as well as to implement and operate a prototypical testbed facility to offer initial evaluation services which are mandatory for the accreditation from a European security authority.”*



Deutsche Telekom Global Business Solutions Belgium NV/SA  
(DTGBS, including Deutsche Telekom Security GmbH and Deutsche Telekom Technik GmbH)

### FULL PARTNERS



AIT Austrian Institute of Technology GmbH (AIT)



**Thales SIX GTS France**  
(TSGF, including Thales Alenia Space France and Thales Belgium)



# NOSTRADAMUS APPROACH



**Widely diversified consortium for a holistic view**

Partners part of PETRUS team, led by DT – 26 NatQCI and 6 Industry projects

Use cases providers in the IRIS<sup>2</sup> SpaceQCI context and QKD companies alliances to align with what the market (will) expect

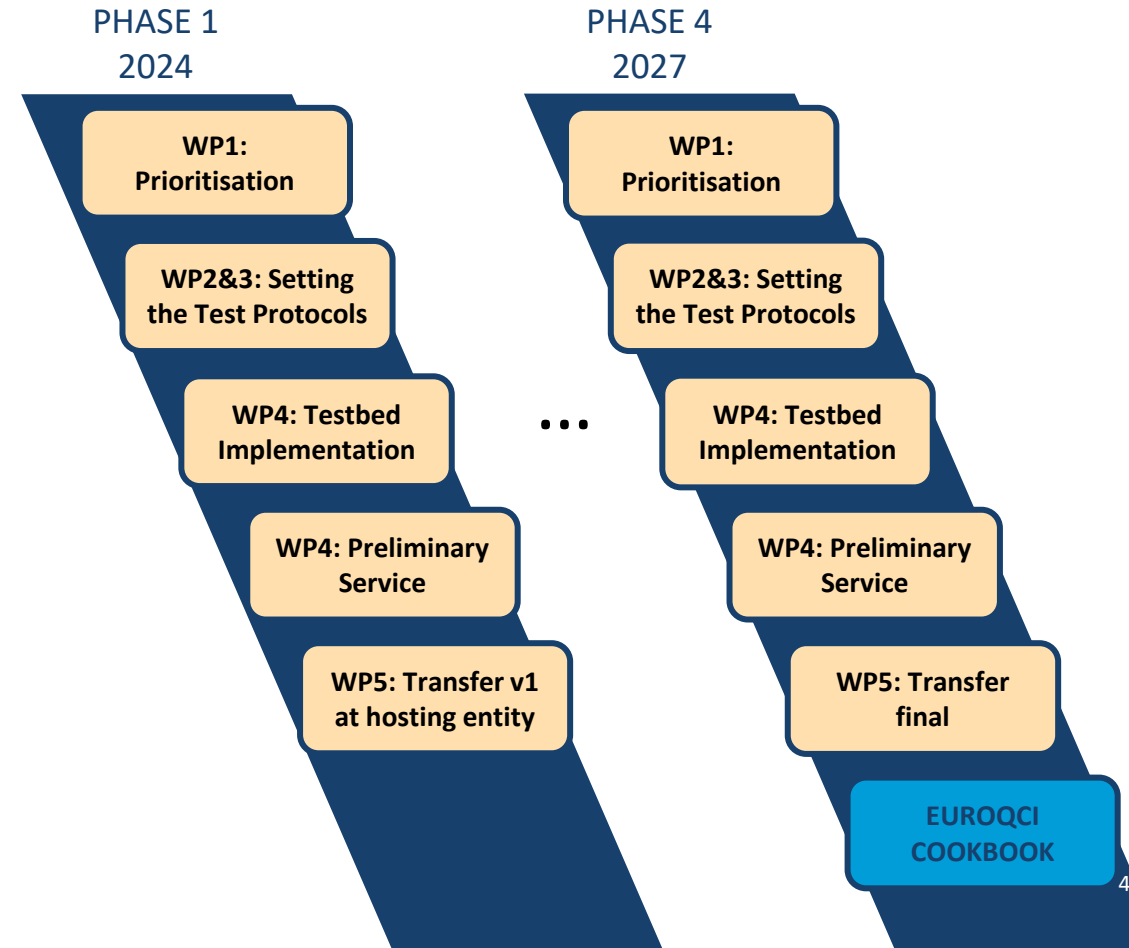
State of the art scientific entities under AIT supervision to implement and validate the functional tests and attacks

Metrology companies to help establish whether the tests can be part of an ISO17025 lab

Licensed ITSEF from DE and FR (DT and Thales) to build the security baseline and the evaluation lab.

Technology transfer experts for the delivery of the lab and the associated trainings in the Hosting Entity.

## OVER 4 PHASES FROM 2024 -2027



# Methodology and Prioritisation Approach

# Nostradamus Vulnerability Analysis

## Construct matrix of all published

- Side Channel Attacks
- Counter Measures

## Insight

- Some counter measures help against several attacks
- Some attacks can be countered by several counter measures

## Results

- 6 general side-channel attacks against DV and CV QKD Systems
- 6 side-channel attacks against CV QKD Systems
- 34 side-channel attacks against DV QKD Systems
- 11 vulnerabilities
- 98 counter-measures in literature

Counter Measures

	1	2	3	4
a	X		X	
b		X		
c		X		
d				X
e	X			
f			X	X
g		X		

Side Channel Attack

# Nostradamus three steps for priority setting

## 1. Step

- No consideration of side-channel attacks against Entangled or MDI QKD Systems

## 2. Step

- No consideration of side-channel attacks not relevant for EU27 systems

## 3. Step

- Expert discussion on feasibility of implementing the side-channel, of feasibility to implement the countermeasures and the sufficiency to implement the counter measures

Counter Measures

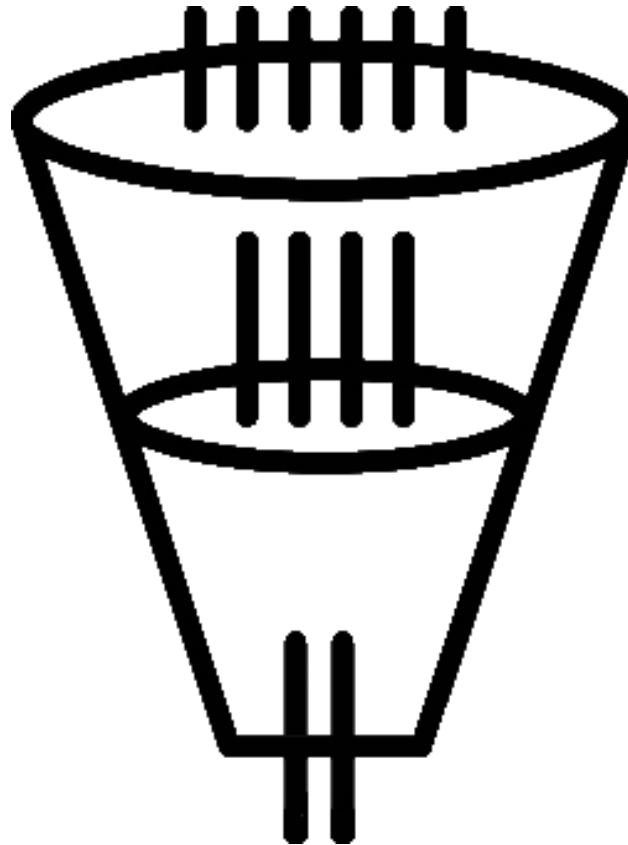
	1	2	3	4
a	X		X	
b		X		
c		X		
d				X
e	X			
f			X	X
g		X		

Side Channel Attack

# Nostradamus Prioritization Approach

## Attack Feasibility

- **Demonstrated**  
the attack has been implemented in the past
- **Viable**  
all the components necessary to implement the attack are currently possible
- **Speculative**  
at least one of the components necessary to implement the attack is currently unavailable
- **Theoretical** for at least some part of the attack it is unclear what physical components are necessary to implement it



## Sufficiency of Counter Measures

- **Closes side-channel**  
sufficient to avoid attack success
- **Impedes attack**  
co-dependent with additional counter measure, e.g health monitoring
- **Unknown efficiency**  
counter measure proposed in literature
- **Shown insufficient**  
CM proposed in literature but already shown not to help

# Evaluation & Certification

# Security Assurance by Evaluation

*specify assurance level*

Developer /  
Applicant

- Produces Target of Evaluation (TOE)
- Documentation of TOE and development processes

Common Criteria  
Approval Schemes  
EUCC

- Checks reports, asks for evidence, issues certificate

NCSA / Certification  
authority

Accredited Lab /  
Evaluator

- Audit, Testing, Vulnerability analysis, Evaluation Reports

# QKD-Specific CC security evaluation standards

**ISO/IEC 23837 (2023): Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution**

- Part 1: Requirements
- Part 2: Evaluation and testing methods

Work 2018 – 2023, Prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, SC 27, Information security, cybersecurity and privacy protection

**ETSI GSQKD016: Quantum Key Distribution (QKD); Common Criteria Protection Profile Pair of Prepare and Measure Quantum Key Distribution Modules**

Work 2020 – 2022, Sponsored and contributed to by German Federal Office for Information Security (BSI), initiated and contributed to by ETSI ISG QKD, authored by Deutsche Telekom Security

2022 – 2023 Under evaluation by SGS Brightsight

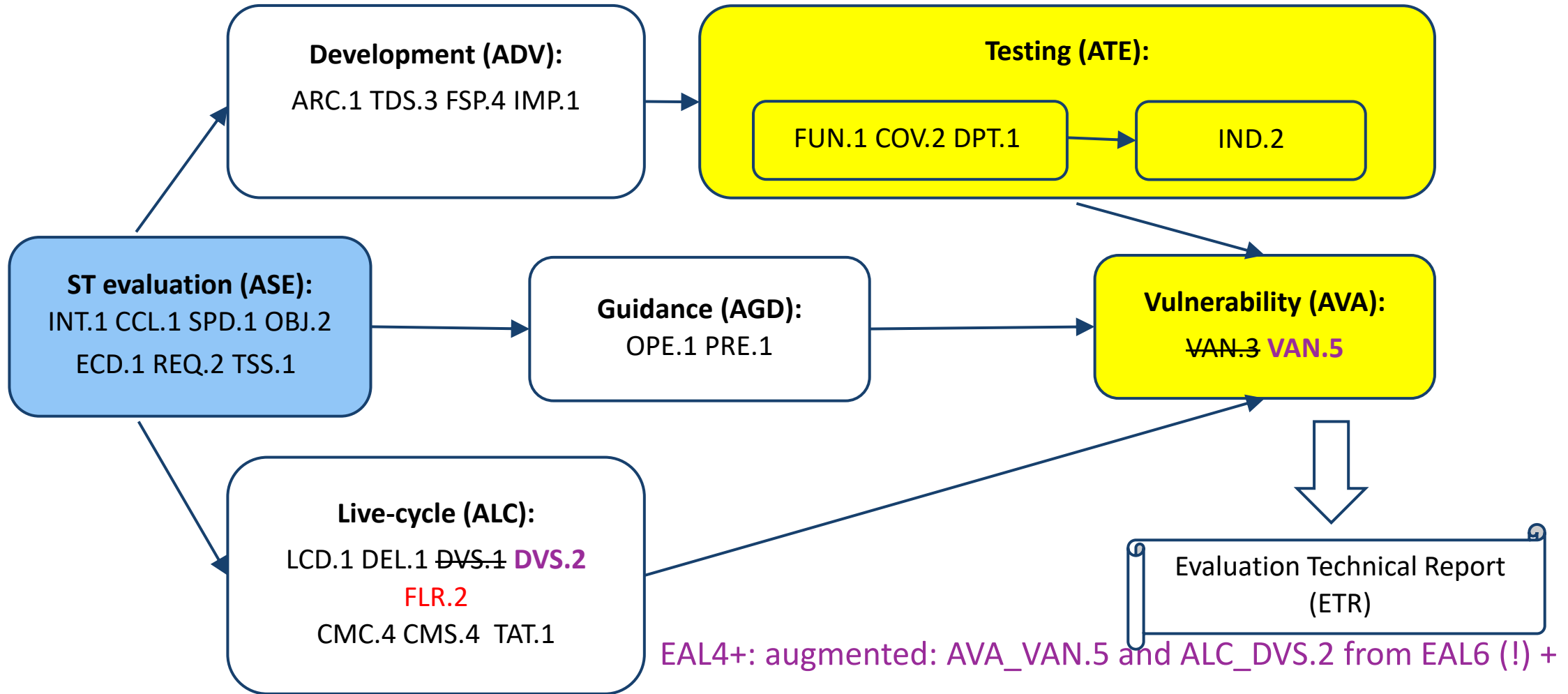
2024 Certified by BSI

**No Technical domain yet for QKD : to be determined by NSAs + migration to CSA/EUCC context**

# Testing in the context of Security Evaluation

# CC Security evaluation process

Perform work units on Security Assurance Requirements (SAR), Example for Evaluation Assurance Level (EAL) 4+.



# Testing activities

## Functional testing of security functions (ATE)

- Review developer evidence in terms of functional testing and perform some independent tests (ATE\_IND) to verify developer's claims or detect issues
- On the quantum channel of a QKD device, it includes testing the efficiency of countermeasures against side channels => Non-standard equipment & methods needed
- Nostradamus will develop Testing capability

## Vulnerability Analysis and Security (robustness) Testing

- Based on a Test Plan (outcome of design review, functional testing and guidance review)
- During QKD devices evaluation for certification: all attacks will be considered
- Most of them are already known by labs & CBs (software stacks, networks, secure packaging...)
- Nostradamus only focus on the "new" ones which are Side Channel Attacks on the Quantum Channel

# Conclusion & Challenges ahead

# Nostradamus will develop the product security baseline

## **For Accreditation**

- A proposition to NSAs of mapping between accreditation level and product certification level

## **For Certification and product manufacturers**

- Protection profiles to be certified by NSAs to support QKD product manufacturers
- The foundations of a future technical domain (or addon to an existing one) with an attack catalogue

## **For Evaluation**

- State of the art matrix "countermeasures vs attacks" to ease design review & vuln. analysis
- The only technical capability lacking across Europe : Tools & techniques to attack the quantum link

# Nostradamus will not

**Redevelop capabilities that already exist (such as testing a network equipment)**

**Deal with testing free space QKD – Focus on terrestrial / fiber QKD**

**Evaluate devices applying for certification – Focus on the quantum link of the test vehicles**

# Challenges

- **Quantum Hacking**
  - Rather new field, not many (European) researchers did focus on it yet
  - Some attacks (and counter measures) have only been described on paper
  - Required equipment is oftentimes not commercially available yet or must even be developed
  - Accessibility of 'Test Vehicles' not guaranteed

# Questions & Discussion



**End of presentation**

# Version History

Date	Version	Responsible	Changes
17.01.2024	1.0	F. Wissel	Initial Version
02.05.2024	1.1	M. Stierle	Final Version