ETSI
The Standards People

Security Conference

Towards certification of Quantum Communications: an EU perspective

Presented by: Adam M. Lewis

European Commission

17th October 2023

Towards certification of Quantum Communications: an EU perspective

Adam Lewis
European Commission Joint Research Centre

- ETSI CybersecurityConference
  Sophia Antipolis, 17th October 2023

Joint
Research
Centre

Why is the European Commission interested ?

- Aligns with EU policy on cybersecurity certification in general
- Required for the European Quantum Communication Infrastructure
- Required for using quantum comms. in EU institutional systems
- Helps to foster a European quantum industry and EU economic security

OL(0

European Commission

Slide 3

OL(0 EU strategic autonomy

OLISLAGER Laurent (CNECT); 2023-10-10T13:32:48.652

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

OL(0

- European Cybersecurity Certification Scheme on Common Criteria
- European Certification Scheme for Cloud Services
  - European Cybersecurity Certification Group NSA/NCSA's (plus others)
- European Cybersecurity Certification Scheme for 5G
  - Conformity Assessment Bodies (CABs)

Regulation (EU) 2023/588 of 15/03/2023 establishing the Union Secure Connectivity Programme

Council Decision of 23/09/2013 on the security rules for protecting EU classified information (2013/488/EU).

Slide 4

OL(0 Add ref, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework?
OLISLAGER Laurent (CNECT); 2023-10-10T13:33:34.330

OL(0

EuroQCI the European Quantum Communication Infrastructure

Artist's view of a European Quantum Communication Infrastructure

- Space and ground segments
- Owned by EU/Member states
- Linked with IRIS^2 (later)

https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

European Commission

Slide 5

OL(0 Beyond the use cases, add general description of EuroQCI (space/ground+terrestrial infra, EU/MS-owned)

OLISLAGER Laurent (CNECT); 2023-10-10T13:34:38.561

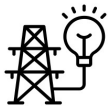
EuroQCI the European Quantum Communication Infrastructure

Use Cases

- Telecommunication

- Transport

- Finance



- Energy

- Health

- Space assets

- Water

- Emergency/disaster response infrastructure

- Cyber Security Operation Centres

Quantum Key Distribution is first service

European Commission

The EC studies for EuroQCI

QCI4EU

KE(1

- 19 Feb to 25 Nov 2020

OQTAVO

- 6 Feb to 27 Nov 2020

QCI4EU – QSAFE

KE(0

- 26 Mar 2021 to 26 Jul 2022

- 1 Apr 2021 to 28 Jul 2022

Slide 7

KE(0 Could be removed to do as for OQTAVO
KLECHA Emilie (CNECT); 2023-10-09T12:16:12.854

KE(1 Put the title as for QoSAC as well or remove the title from QoSAC
KLECHA Emilie (CNECT); 2023-10-09T12:16:54.183

EuroQCI Testing and Evaluation infrastructure

- Call for Tenders open 5th July – 29th August 2023
- 4 year project, 16 M€ funding from Digital Europe Programme
- Proposal evaluation completed 18th September

1) Prioritization for sequencing of tests, QKD protocols and side-channel threats

2) Definition of Test Protocols

3) Definition of Product Security Baseline

4) Initial operation of a testing and evaluation facility

5) Transfer of the testbed to a hosting entity selected by EC

European Commission

Slide 8

KE(0 Procurement to be specified call refers often to a grant
KLECHA Emilie (CNECT); 2023-10-09T12:17:42.942

KE(1 Before this I think could be useful to have a slide on the overall implementation of the terr part at least with the DEP projetcs before going through the procurment
KLECHA Emilie (CNECT); 2023-10-09T12:18:47.148

OL(1 0 Agree
OLISLAGER Laurent (CNECT); 2023-10-10T13:41:59.198

KE(2 It may open the door on the security baseline where I'm not sure we want to go in the context of the conference
KLECHA Emilie (CNECT); 2023-10-09T12:19:38.248

OL(2 0 It is part of the list of tasks from the tender specs.
OLISLAGER Laurent (CNECT); 2023-10-10T13:42:23.136

OL(3 TED publication date was 5/7, see https://etendering.ted.europa.eu/cft/cft-display.html?cftId=14339. General guideline for these slides, since the evaluation results are not yet out (not even whether the call will lead to a project), restrict info to what is publicly available at that page.
OLISLAGER Laurent (CNECT); 2023-10-10T13:36:31.875

OL(4 Worth mentioning the estimated value, 16M€
OLISLAGER Laurent (CNECT); 2023-10-10T13:36:57.714

OL(5 And closed 29 August
OLISLAGER Laurent (CNECT); 2023-10-10T13:37:09.349

OL(6 Is it a "project" for a procurement?
OLISLAGER Laurent (CNECT); 2023-10-10T13:38:29.911

OL(7 List is from the technical specifications, fine. Add 6: Document operation, maintenance, training...
OLISLAGER Laurent (CNECT); 2023-10-10T13:41:42.048

OL(0

ISO/IEC 17025 Testing and calibration laboratories

Protection Profile

ETSI GS QKD 016

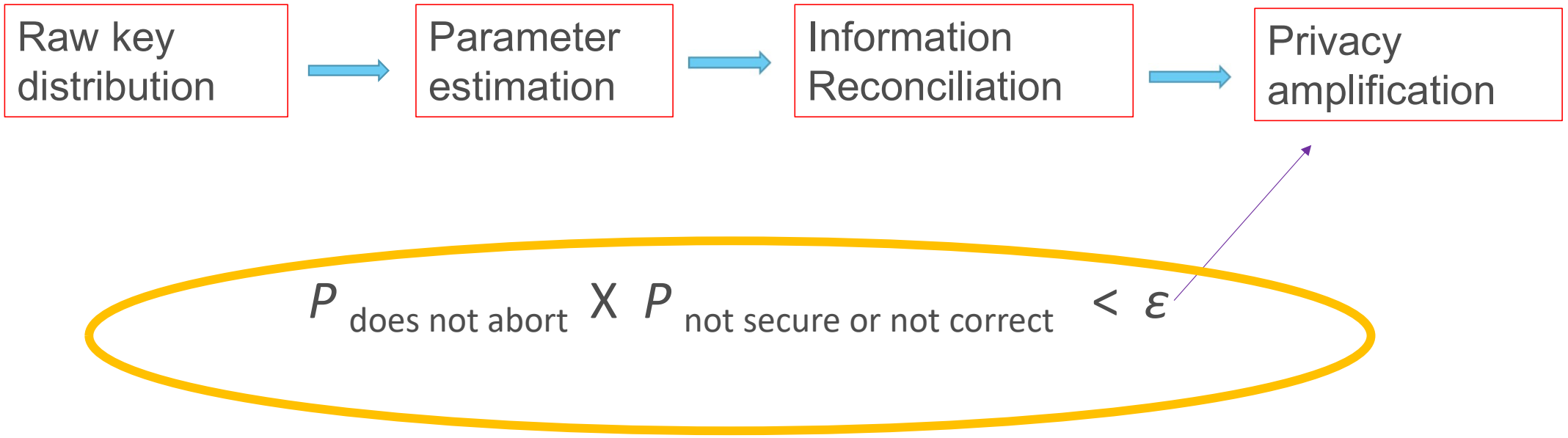
ISO/IEC 15408 - Common Criteria

Slide 9

OL(0 Add some context in this slide?

OLISLAGER Laurent (CNECT); 2023-10-10T13:42:57.743

Generic QKD security – (over) simplified



Security Proof

Test subsystems or test components?

QKD products

Transmitter Module
Receiver Module
Key Management System
Trusted QKD node
Network Controller

Application interface
Interfaces within standard optical networks

OL(0

Components

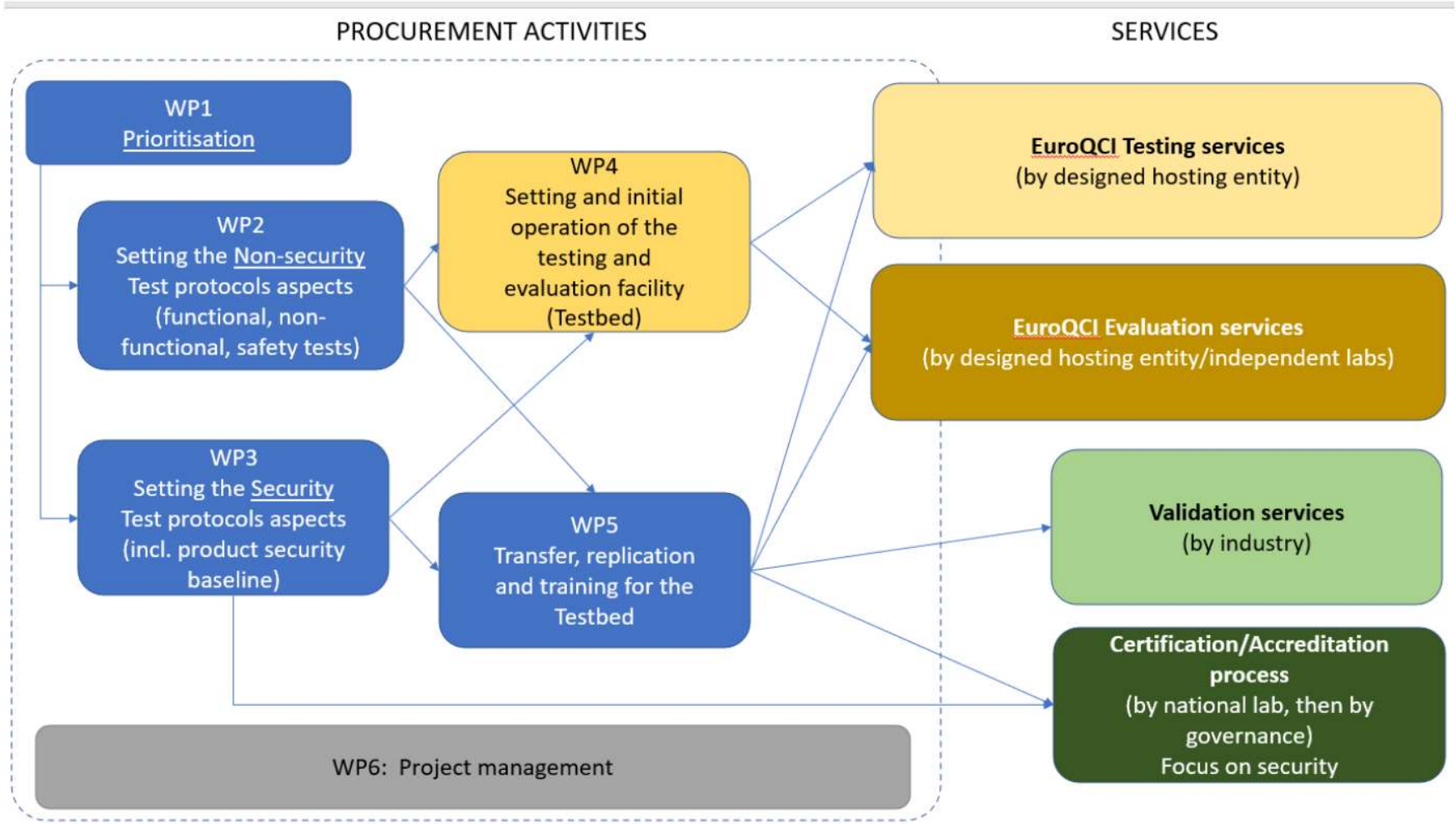
- Photon detector (avalanche photodiode /superconducting nanowire)
- Attenuated laser diode or single-photon source
- Intensity modulator
- Beam splitter
- Polarising beam splitter
- Variable optical attenuator
- Optical isolator
- Narrow band pass optical filter
- Delay line
- Monitoring detector
- Electronic polarisation controller
- Fibre stretcher
- Self-differencing circuit
- Fibre-optic isolators
- Fibre-optic circulators
- Synchronization devices
- Phase stabilizers

OL(0 Add source: SPD or attenuated laser

OLISLAGER Laurent (CNECT); 2023-10-10T13:44:56.408

Non-exhaustive list of side-channel attacks

Intercept and resend
Man-in-the-middle
Photon number splitting
Bright-light denial-of-service
“Trojan horse” (interrogating pulse)
Multi-photon emission
Imperfect encoding
Fault injection
Phase correlation between signal pulses
Efficiency mismatch
Time-shift
Back-flash
Manipulation of local oscillator reference of CV-QKD
Anti-countermeasure
Physical breach of the QKD module


PROCUREMENT ACTIVITIES
SERVICES
WP1
Prioritisation
WP2
Setting the Non-security
Test protocols aspects
(functional, non-
functional, safety tests)
WP3
Setting the Security
Test protocols aspects
(incl. product security
baseline)
WP4
Setting and initial
operation of the
testing and
evaluation facility
(Testbed)
WP5
Transfer, replication
and training for the
Testbed
WP6: Project management
EuroQCI Testing services
(by designed hosting entity)
EuroQCI Evaluation services
(by designed hosting entity/independent labs)
Validation services
(by industry)
Certification/Accreditation
process
(by national lab, then by
governance)
Focus on security

Thank you

European Commission