

Integrated Project Cyber security of energy systems for the digital-energy transition

An integrated framework for evaluating standard-based and quantum-safe cybersecurity solutions for electrical energy applications

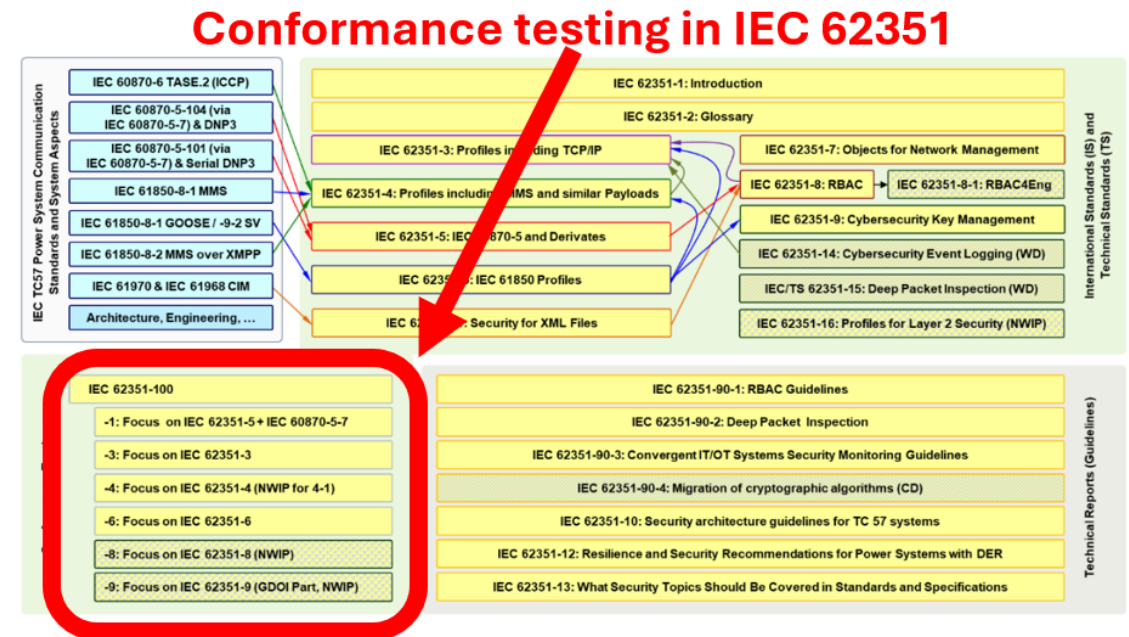


- The CYSPEC framework for performance evaluation and conformance assessment of cybersecurity solutions in the electrical-energy sector.
- Quantum-safe solutions, both post-quantum cryptography (PQC) and quantum technologies (QKD)
- Specification of conformance test procedures for the Charging Infrastructure Controller (CIR)

Goal:

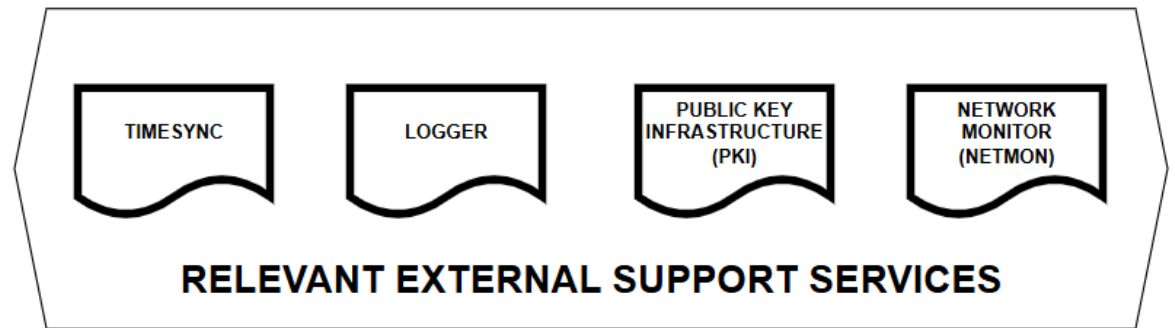
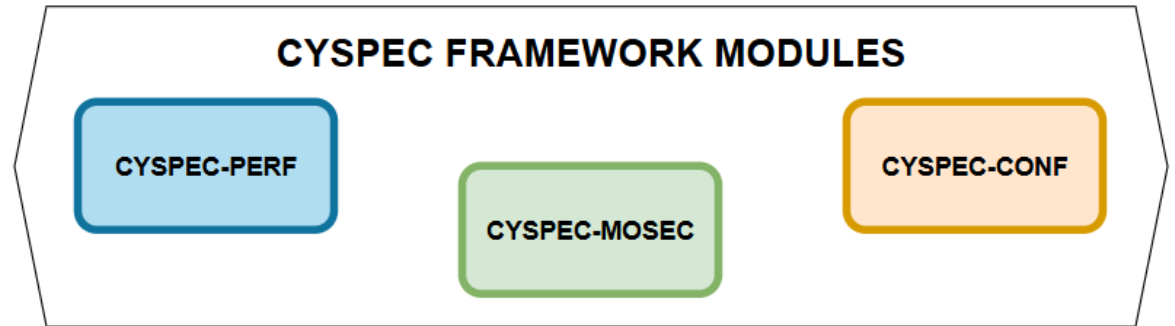
- develop a software framework (CYSPEC) able to support the **evaluation** of the **performance** of devices and solutions in the electrical-energy sector in terms of:

- **overhead** introduced by **cybersecurity** (e.g., IEC 62351-3)
- **compliance** with sector **standards** related to **cybersecurity** of telecommunications (e.g., IEC 62351-100-3)



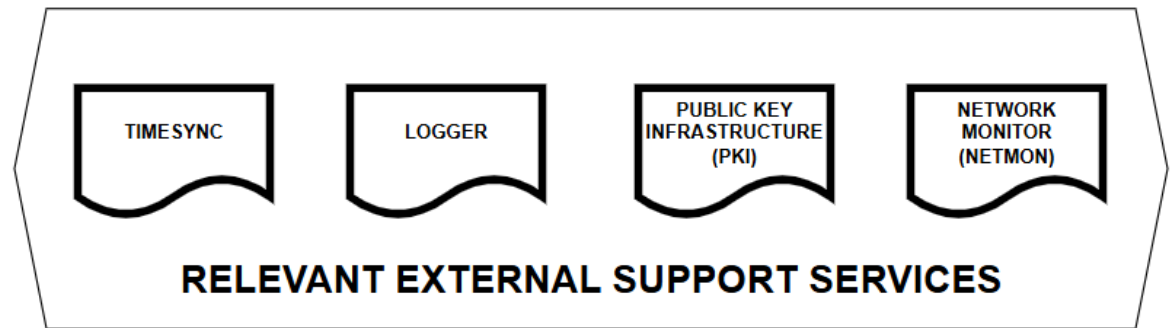
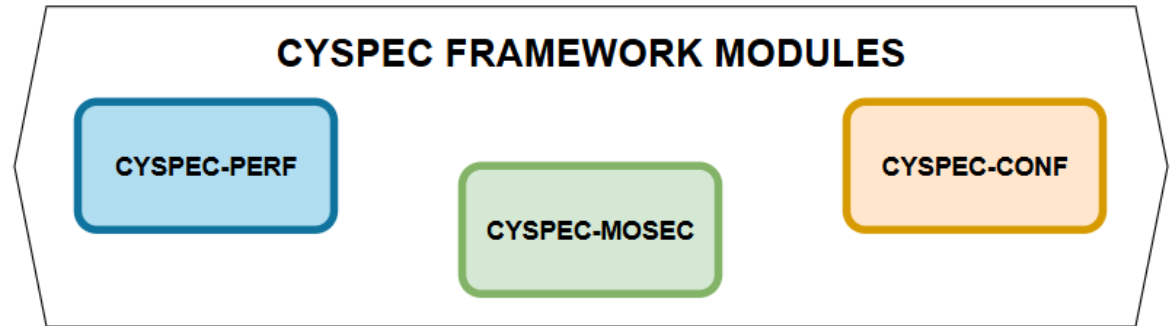
Modules:

- **CYSPEC-PERF:**
 - Measurement of the impact of algorithms and parameters on performance (e.g. latency, jitter, overhead, ...)
- **CYSPEC-CONF:**
 - Evaluation of the compliance of implementations with standard requirements
- **CYSPEC-MOSEC:**
 - Coordination, monitoring, control, setup



External services:

- **TIMESYNC:**
 - synchronization of modules, subcomponents, and services
- **LOGGER:**
 - log collection and management
(both from the framework and from tested solutions)
- **PKI:**
 - management of the digital-certificate lifecycle
- **NETWORK MONITOR:**
 - network sniffer, switch with mirroring capabilities





SyncServer S600
NTP and PTP stratum 1



Management



NTP - PCS-ResTest LAN



PTP - PCS-ResTest LAN - Power C37.238 2017 Profile



NTP - Wider range of LAN/WANs of RSE



PTP - Wider range of LAN/WANs of RSE - Telecom 2008 Profile

```
ptp4l[12873796.483]: master offset -42527 s2 freq -27104 path delay 187422
ptp4l[12873797.483]: master offset -14577 s2 freq -24323 path delay 168400
ptp4l[12873798.483]: master offset -8937 s2 freq -23768 path delay 163750
ptp4l[12873799.483]: master offset -31235 s2 freq -26029 path delay 163750
ptp4l[12873800.483]: master offset 891 s2 freq -22816 path delay 157452
ptp4l[12873801.483]: master offset -26735 s2 freq -25605 path delay 155395
ptp4l[12873802.483]: master offset 5874 s2 freq -22338 path delay 155395
ptp4l[12873803.483]: master offset -1246 s2 freq -23052 path delay 155578
ptp4l[12873804.483]: master offset 3511 s2 freq -22572 path delay 155578
ptp4l[12873805.483]: master offset -3321 s2 freq -23259 path delay 155578
ptp4l[12873806.483]: master offset 708 s2 freq -22855 path delay 155578
ptp4l[12873807.483]: master offset 120477 s2 freq -10758 path delay 155578
ptp4l[12873808.483]: master offset -21467 s2 freq -24974 path delay 156659
ptp4l[12873809.483]: master offset -10725 s2 freq -23910 path delay 156659
ptp4l[12873810.483]: master offset 58851 s2 freq -16894 path delay 156659
ptp4l[12873811.483]: master offset -42507 s2 freq -27072 path delay 156659
ptp4l[12873812.483]: master offset -8263 s2 freq -23656 path delay 155578
ptp4l[12873813.483]: master offset -9201 s2 freq -23759 path delay 154973
ptp4l[12873814.483]: master offset -47899 s2 freq -27677 path delay 154170
ptp4l[12873815.483]: master offset 28195 s2 freq -20039 path delay 154170
ptp4l[12873816.483]: master offset -5304 s2 freq -23394 path delay 158861
ptp4l[12873817.483]: master offset 10747 s2 freq -21779 path delay 158861
ptp4l[12873818.483]: master offset -12023 s2 freq -24068 path delay 166302
ptp4l[12873819.483]: master offset -3641 s2 freq -23233 path delay 166302
ptp4l[12873820.483]: master offset -698 s2 freq -22939 path delay 161616
ptp4l[12873821.483]: master offset -439 s2 freq -22914 path delay 162663
```

Wider accessibility to time synchronization for:

- PCS-ResTest lab
- other labs and facilities of RSE



- Protocol Buffers (Protobuf) for structured message definition and efficient binary serialization.
 - Ensures strong typing, forward/backward compatibility, and cross-platform data exchange.
- ZeroMQ as the asynchronous messaging system connecting the modules (PERF, CONF, MOSEC).
 - Supports publish/subscribe, request/response, and pipeline patterns; high scalability; broker-less architecture.



CYSPEC_PERF_SETUP, CYSPEC_PERF_SETUP_STATUS, CYSPEC_CONF_SETUP, CYSPEC_CONF_SETUP_STATUS, CYSPEC_SYNC_TIME,
CYSPEC_SYNC_TIME_STATUS, CYSPEC_NETMON, CYSPEC_NETMON_STATUS, CYSPEC_TEST_RUN, CYSPEC_TEST_RUN_STATUS, CYSPEC_TEST_RESULTS

Q-day: availability of a cryptographically relevant quantum computer

- estimated: 5–10 years

Cryptography:

- symmetric (AES): Grover's algorithm
 - mitigation feasible: increase key length
(AES-128 \Rightarrow weak, AES-256 \Rightarrow safe)
- asymmetric (key exchange: RSA/DH/ECDH/ECDHE): Shor's algorithm
 - key-length increase not beneficial
- asymmetric (digital signatures: RSA/DSA/ECDSA/EdDSA): Shor's algorithm
 - key-length increase not beneficial

NIST Standards:

- ML-KEM (Kyber) → key exchange
- ML-DSA (Dilithium), SLH-DSA (SPHINCS+) → digital signatures, FN-DSA (Falcon) coming
- HQC selected as alternative KEM (standard expected \approx 2027)

Trade-offs vs classical algorithms:

- Larger keys / signatures
- Performance

Performance aspects vary:

e.g.

- Falcon: smaller signatures
- Dilithium: fast
- SPHINCS+: small keys but large signatures

Software libraries:

- NIST PQC Library: official NIST codebase for PQC candidates
- Liboqs: open-source C library from the Open Quantum Safe project(PQC key-exchange + signatures)
- PQClean: portable, readable, secure C implementations of PQC algorithms

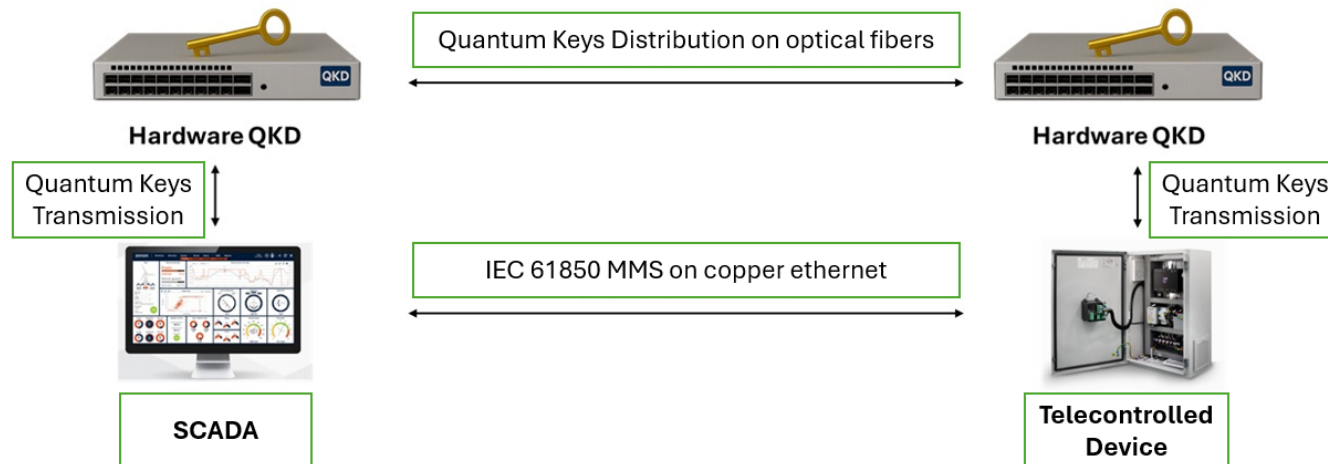
Collaboration with Leonardo S.p.A.

Goal:

- integration of QKD devices to protect telecontrol communications

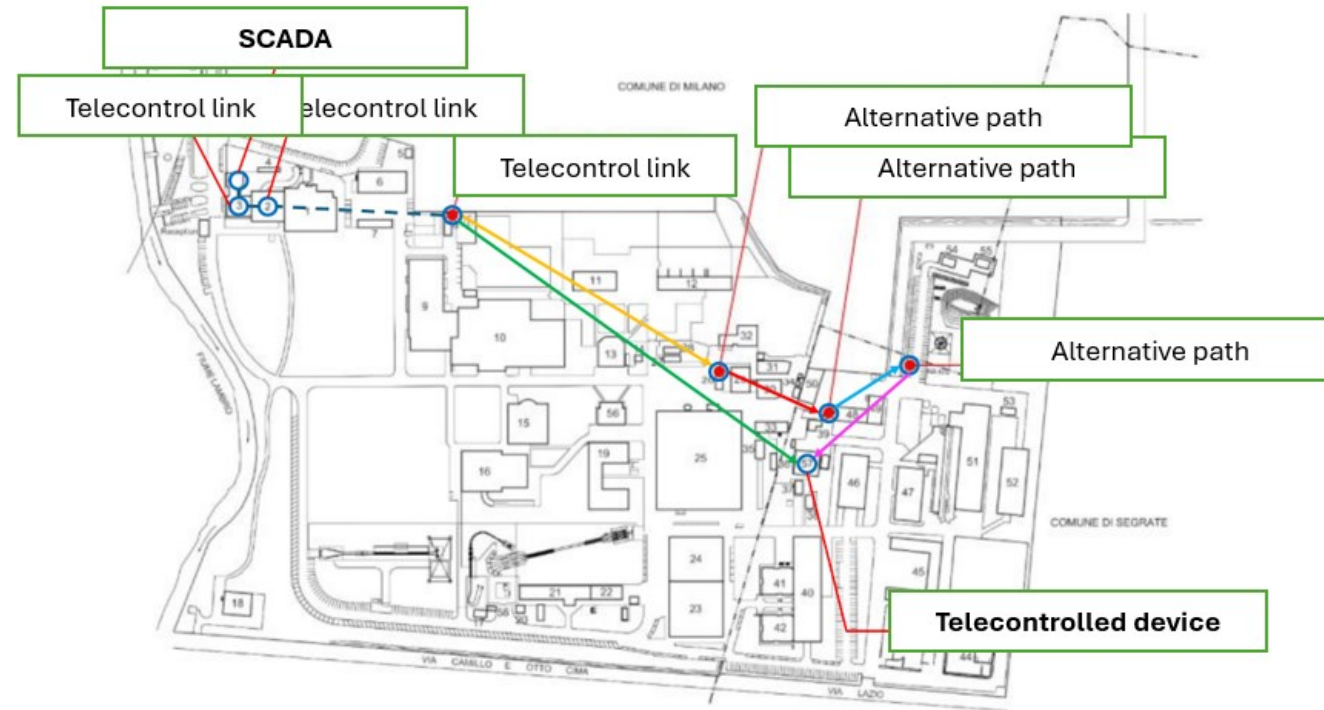
Activities performed:

- identification of the use case



Activities performed:

- preliminary feasibility assessments
- state-of-the-art quantum solutions, constraints and applicability



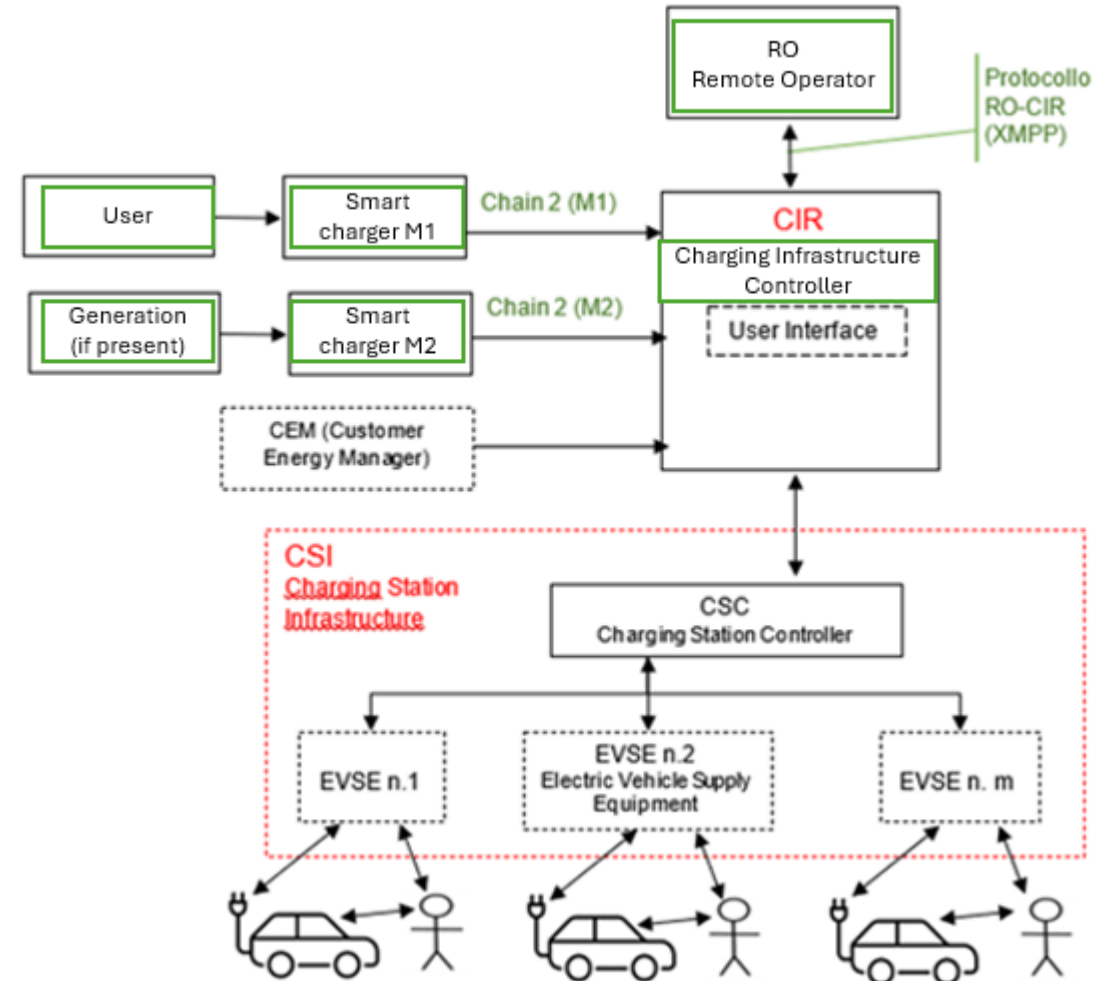
The CIR (CEI 0-21; CEI PAS 57-127):

- power-draw data collection
- data exchange with the RO
- dynamic power regulation

Experimentation completed in 2024 with involvement of:

- device manufacturers
- RO

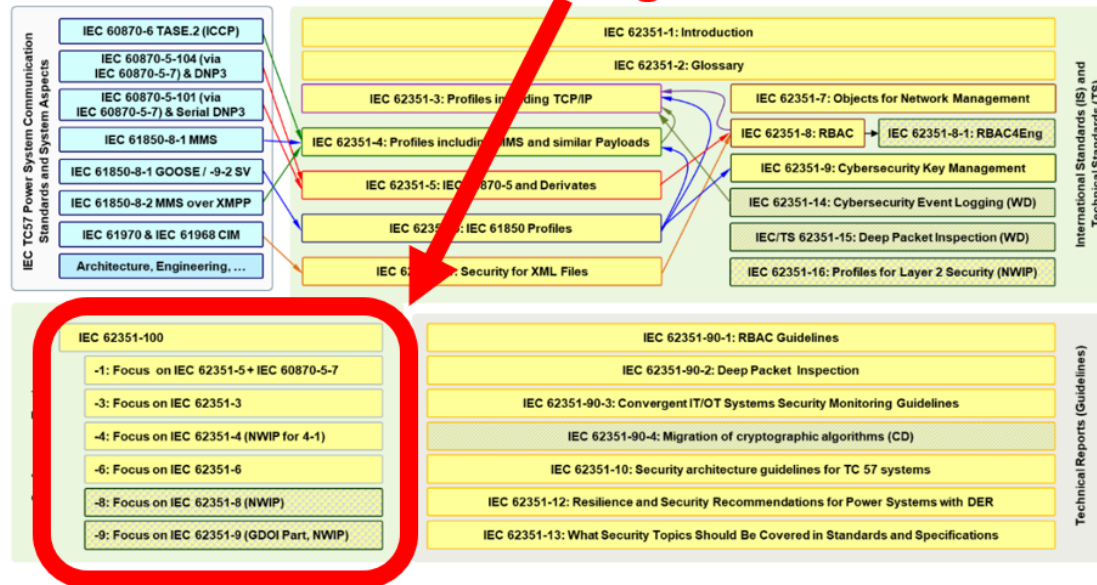
Reference architecture for CIR communication interfaces – Annex X of CEI 0-21;V1



Contribution to updated Edition 2 of CEI PAS 57-127

- Specification of “what to verify” for cybersecurity conformance assessment

Conformance testing in IEC 62351



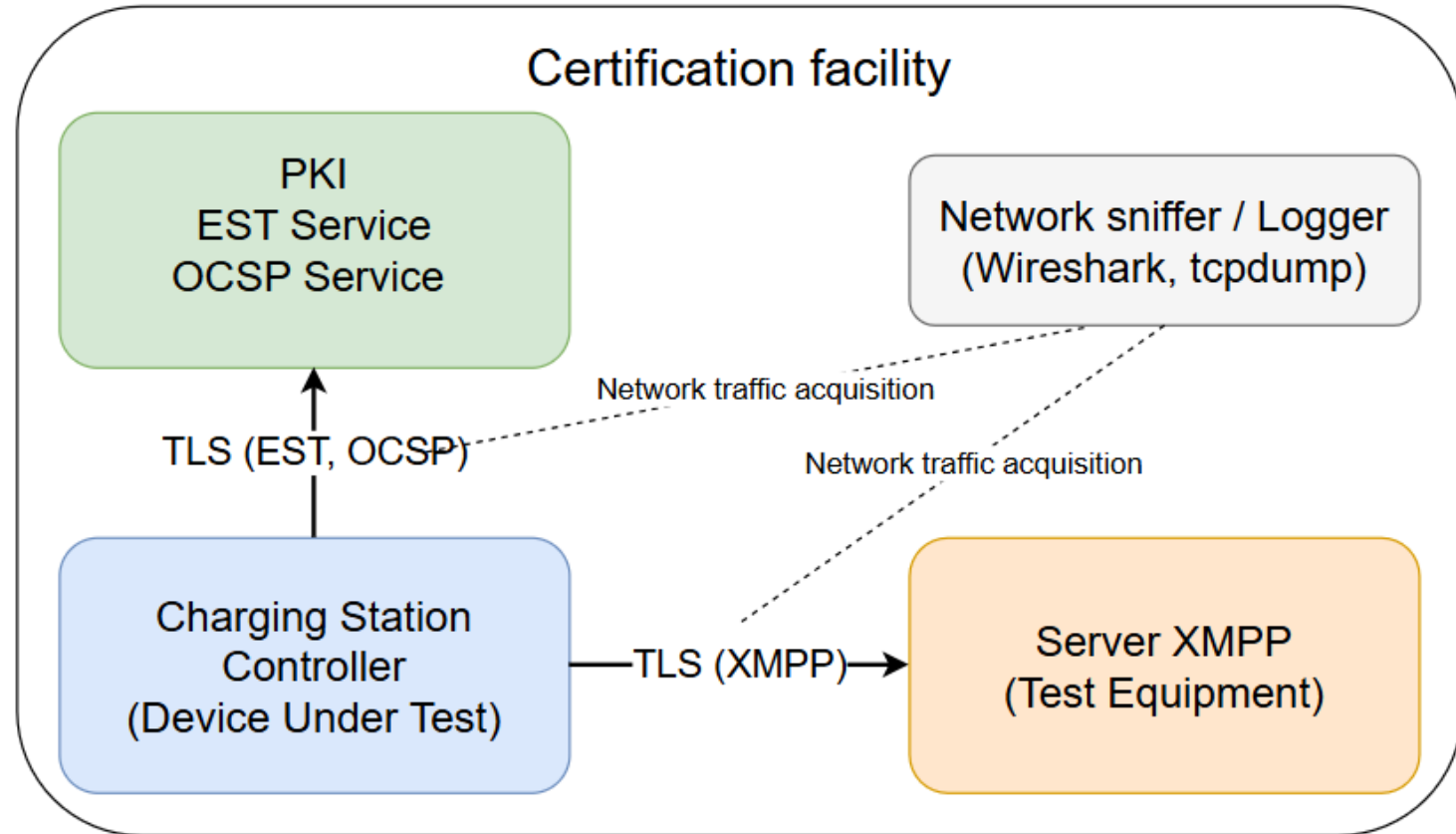
Description	Topic
Check that the CIR contacts the PKI /cacerts endpoint and stores the Explicit TA	DIGITAL CERTIFICATES
Check that the CIR generates a CSR containing the JabberID in the SAN-XmppAddr field	DIGITAL CERTIFICATES
Check that the CIR sends the CSR to the /simpleenroll endpoint authenticating with its pre-enrollment certificate and stores the returned certificate	DIGITAL CERTIFICATES
Check that, before expiration, the CIR requests certificate renewal at /simpleenroll using the expiring certificate	DIGITAL CERTIFICATES

Cybersecurity (CEI PAS 57-127 Ed. 2):

Description	Topic
CIR establishes a connection to the XMPP server using configured IP and TCP port	TCP CONNECTION
CIR supports the STARTTLS method	XMPP
CIR supports TLS 1.2	TLS VERSION
If available, TLS 1.3 can be enabled/disabled via configuration parameter	TLS VERSION
CIR validates TLS certificate (time validity, issuing CA, digital signature, identity)	DIGITAL CERTIFICATES
CIR manages digital certificates up to maximum allowed size	DIGITAL CERTIFICATES
CIR allows configuration of minimum required trust anchors	PKI
CIR supports CRL and OCSP	PKI
CIR supports all mandatory TLS cipher suites	TLS
CIR supports RSA and ECDSA key sizes as required	DIGITAL CERTIFICATES
CIR supports SASL EXTERNAL authentication	XMPP
CIR terminates the XMPP connection when only parameters below minimum requirements are proposed	XMPP

From “what to verify” to “how to verify”:

- prerequisites
- required instrumentation
- step-by-step procedure
- termination criteria



- We are developing the CYSPEC framework to support performance evaluation and conformance assessment of cybersecurity solutions in the electrical-energy sector.
- We have started exploring quantum-safe solutions, including both post-quantum cryptography (PQC) and quantum technologies (QKD), with the goal of enabling their future integration into the CYSPEC environment (performance, conformance evaluations).
- We carried out a detailed activity on the specification of conformance test procedures for the Charging Infrastructure Controller (CIR), addressing not only the normative “what to verify” but also the “how to verify” for practical realization (CYSPEC or certification body).

Thank you for the attention

maurogiuseppe.todeschini@rse-web.it, elsa.corniani@rse-web.it