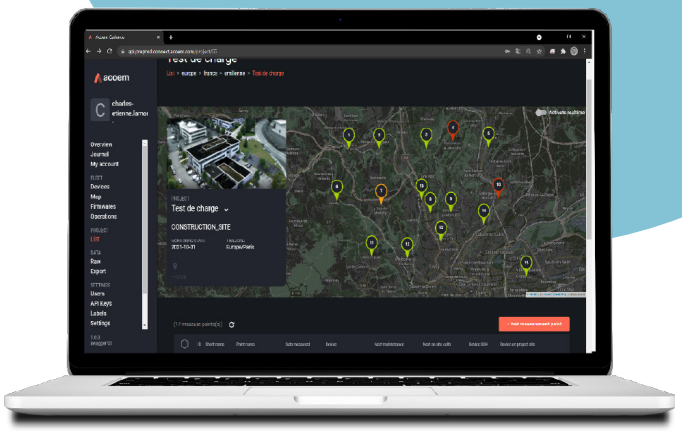
Cadence

NOISE MONITORING AND MANAGEMENT SOLUTION



Secured by design

- All security standards are implemented. Communications are encrypted by default
- The services are exposed through a reverse proxy & a load balancer

Interoperability

- All communications between services are based on a documented API (OpenAPI standard)
- Cadence is able to connect to third party APIs or be consumed by third parties through APIs.

Scalability & redundancy

- The service is able to allocate more resources to manage a peak load without degrading the user experience
- The service is running in at least 3 different locations to ensure availability.

Cadence is hosted by a Public Cloud Provider with the following characteristics

ISO/IEC 27001/27017/27018/27701,

SOC 1/2/3, PCI DSS, and FedRAMP certifications,

Alignment with HIPAA, GDPR and CCPA.

Cadence is proposed by Acoem

Headquarter based at Lyon in FRANCE

Certified ISO/IEC 9001:2015, 14001 and GDPR compliant

Acoem Business Cloud Security policy available on demand*

ISO/IEC 27001

ISO/IEC 27017

ISO/IEC 27018

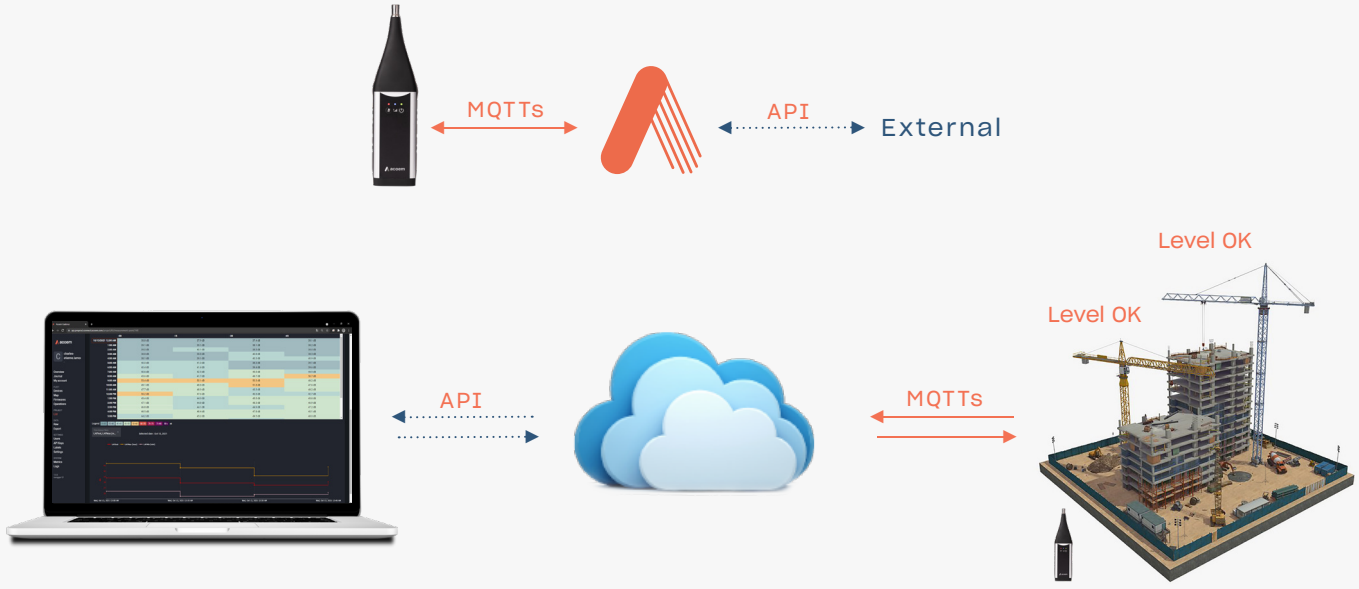
SOC 1/2/3

PCI DSS

CSA STAR

MQTTs - Message Queuing Telemetry Transport Secured: All communication between devices and Cadence platform are using MQTTs with TLS -Transport Layer Security - encryption to protect the transferred information against interception, modification or forgery.

API - application programming interface: all APIs are exposed through HTTPs with TLS encryption to protect the transferred information against interception, modification or forgery.



NOT1595 OCTOBER 2021 A

acoem
CREATING ENVIRONMENTS OF POSSIBILITY