

## **DESCRIPTION OF THE DIGITAL SECURITY AND CONNECTIVITY FEATURES WITH REGARD TO PHYSICAL AND DIGITAL INFRASTRUCTURE**

*in particular those allowing EUCA to comply with relevant cybersecurity standards and legislation and for all core facilities to implement certified protocols for end-to-end encryption of data, enforce access controls and deploy advanced systems for continuous issue detection, timely reporting and effective response.*

Regarding the requirements set out in point 23), it should be noted that the location that will host EUCA must have an integrated digital and physical infrastructure that ensures operational continuity, data confidentiality and resilience to threats.

The security system must comply with international standard ISO/IEC 27001 – Information security management systems, and international standard ISO/IEC 27002 – Information security controls, with Directive (EU) 2022/2555 (known as NIS2) on measures for a high common level of cybersecurity across the Union, and with Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR).

Therefore, in addition to the establishment of a SOC for continuous security event monitoring, log management, anomaly detection, and related management, teams and procedures must be implemented for security governance, ongoing user training and awareness, periodic vulnerability assessments, risk evaluation and management, incident response procedures, and auditing. Furthermore, the infrastructure supporting EUCA will be designed according to a 'security by design' and 'Zero Trust' model, with multilayered controls and continuous monitoring.

### **Internal connectivity and network architecture**

The headquarters network will be structured as a highly segmented campus network: separate domains for institutional users, guests, critical services, IoT/OT and security devices. L2/L3 segmentation (VLAN and VRF) will be reinforced by SDN micro-segmentation and next-generation firewalls with application-level inspection. Wired and wireless access will adopt 802.1X *Network Access Control* (EAP TLS) with device/user certificates, endpoint profiling and automatic quarantine of non-compliant devices. Wi-Fi networks will be provided in WPA3-*Enterprise* mode, with physical-logical traffic separation, RF-*monitoring* and completely isolated guest policies. The exit perimeters will be monitored by DLP (*Data Loss Prevention*) systems capable of detecting, blocking and reporting any attempt to exfiltrate data. The “secure room” described in Question 5.1 will constitute a logical domain with the highest level of segregation, with dedicated access and logging policies.

### **End-to-end encryption and key management**

All sensitive data flows will be protected using end-to-end encryption based on TLS 1.3 (with Perfect Forward Secrecy), IPsec for inter-site connections and robust encryption

algorithms such as AES256GCM. For application and messaging channels, mTLS, S/MIME or OpenPGP will be adopted depending on the specific requirements of the use case. Keys will be stored in Hardware Security Modules (HSMs), with institutional PKI, periodic rotation, certificate pinning for critical services, and key escrow regulated by approved procedures. Data at rest will be encrypted on servers, storage devices, and portable devices; escrow policies and secure media destruction mechanisms will be employed. Key rotation will be periodic and automated. For communications between EUCA domains and other institutional domains, encryption solutions of equivalent level will be used, with the possibility of physical/logical segregation of network paths.

### **Enforce access controls and Zero Trust model**

Digital identity will be the new perimeter: multi-factor authentication for all privileged access, identity and access management (IAM/IGA) with roles (RBAC) and attributes (ABAC), *Privileged Access Management* (PAM) with just-in-time, session recording and two-person approvals for high-impact actions. The *Zero Trust* principle requires continuous context verification (user, device, location, risk), endpoint posture assessments, least privilege restrictions and immediate blocking in case of anomalies. All administrative access to EUCA systems will be subject to detailed logging and periodic review, with segregation of duties between system, network, and security administrators.

### **Advanced deployment systems and continuous monitoring**

System, device and application updates will follow DevSecOps pipelines with code signing, Software Bill of Materials (SBOM), integrity checks and canary/bluegreen deployments. The infrastructure will be immutable where possible (golden images, IaC) and governed by *Infrastructure as Code* with *policy as code* and tracked change management. Continuous detection will be based on EDR/XDR on endpoints, NDR on the network and centralised SIEM with SOAR for response automation; UEBA and anomaly detection will be used to identify atypical behaviour. A vulnerability management programme (periodic scanners, patching at defined windows, compensating controls) and threat intelligence with updated use cases are planned. Backups will be encrypted, immutable and offline, in a 3 2 1 logic with regular recovery tests and geographic replication.

### **Physical infrastructure and operational continuity**

The site will implement a multi-factor physical access control system (badge, biometrics), protected perimeters, integrated video surveillance with intrusion detection systems, tamper-proof racks, and, where necessary, electromagnetic shielding measures. For the most sensitive areas, a TEMPEST risk assessment will be conducted through radiation survey measurement campaigns. UPS, backup generators, and redundant cooling solutions will be provided, with disaster recovery plans aligned to business continuity requirements.

The availability of critical EUCA services will be sized to at least 99.99% annually, with RPO/RTO objectives defined based on the different service domains.

### **Incident handling and reporting obligations**

The infrastructure will be equipped with a structured security incident management process, including: 24/7 detection and triage functions based on SIEM/SOAR and specialized teams; documented technical and decision escalation procedures; workflows for the timely notification to relevant authorities (national/European CSIRT) in compliance with the obligations set out in the NIS2 Directive and the national transposition laws; periodic reporting to the involved administrations, with performance indicators (MTTD, MTTR) and root cause analysis.

The combination of the measures described allows EUCA to offer a secure digital platform, continuously monitored, capable of ensuring end-to-end encryption, robust access controls, effective incident detection and response, in full compliance with international standards and European regulations on cybersecurity and data protection.