Join the ACTIVAGE challenge, become an #ACTIVAGER!

www.activageproject.eu
coordinator@activageproject.eu

@ACTIVAGEproject
ACTIVAGE project

ACTIVAGE Security & Privacy achievements

GDPR compliance
Secured Gateway by a dedicated Secure Element device (TPM)
Co-developed within ACTIVAGE by CEA-IRI NanoElec & STMicroelectronics

Protect devices
Security Technologies Provide strong security primitives to protect against malicious firmware upgrade attempts and reverse engineering.

Ensure Secure Communications
Communication encryption is a requirement for IoT devices which may send and receive sensitive and/or personal data. Authentication and strong encryption ciphers protect both your data and privacy.

Enable privacy
Recent adoption of the GDPR makes cybersecurity essential to ensure privacy.

ACTIVAGE Security & Privacy Issues

According to GDPR, IoT technologies bring concerns for initiating and applying core principles, security and privacy tools for handling big data management & processing and sensitive data (Health Data).

To cope with these concerns and comply with GDPR, ACTIVAGE initiated Data Privacy and Security measures:

- Privacy policies and terms:
- Encryption procedures.
- Transparency, Accountability.
- Methods as data minimization and Pseudonymising personal data as soon as possible as defined from the beginning of the project.
- DPIAs assessment carried out according to GDPR.

This proof of concept has been designed to operate the ACTIVAGE IoT devices with high trust based on integrity measurements, memory, and communication encryption.

To protect human rights and ensure data processing in compliance to legal and ethical requirements, ACTIVAGE implemented a number of General practices & Security and Privacy tools:

- ‘Privacy by design’.
- Policy framework in consistency with ethical and legal requirements.
- Privacy Enhancing Technologies (PET’s), as Blockchain technologies.
- Mitigation measures for potential data breach.

Within ACTIVAGE a need emerged for Security & Privacy (S&P) module development that aims to provide a trustful digital environment. Five key principles have been initiated: user and entity authenticity, authorization, integrity, confidentiality and non-repudiation. The S&P Layer implements the following services:

- Access control Management (Identification, Authentication, Authorization and Accountability).
- Sensitive Data Handling & Security Administration requirements.