GreenPowerIT

D6.2 Specification for public procurement

This project has received funding from the European Union's Digital Europe programme under **Grant Agreement No. 101083637**

Deliverable number :	D6.2
Due Date :	30/06/2023
Nature[1] :	Report
Dissemination Level[1] :	Public
Work Package :	WP6
Lead Beneficiary :	CITC
Contributing Beneficiaries :	ALL

DOCUMENT HISTORY

Version	Date	Author	Description
0.1	01.06.2023	CITC	Creation Deliverable template
0.2	07/07/2023	CITC	Updates and completions
0.3	12/07/2023	CITC	Critical review and proofreading
0.4	17/07/2023	CITC	Final edits for approval
1.0	19/07/2023	CITC	Final version

Table of Contents

Acronyms

Acronym	Description
EDIH	European Digital Innovation Hub
IoT	Internet of Things
CCTP	Specification of particular technical clauses
GTC	General terms and conditions
CE marking	An acronym for the French "*Conformite Europeenne*" certifies that a product has met EU health, safety, and environmental requirements, which ensure consumer safety.
ENISA	European Union Cybersecurity Agency

1. Introduction

1.1 Purpose and Scope of this document

The purpose of this document is to define the needs and requirements of the «XYZ» project precisely and comprehensively. Its aim is to establish a structured framework, enabling a common understanding among all involved parties. By clearly defining the objectives to be achieved, risks to be anticipated, as well as technical and environmental constraints, this document will serve as a reference throughout the project, ensuring its success.
The procedure for specifications for public procurement to be followed is illustrated with the following example and should be adapted to each specific case, technology and sector: Development and deployment of environmentally friendly IoT objects incorporating "Secure by Design" security measures.

1.2 References

1. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (accessed on 07/07/2023): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (accessed on 07/07/2023): https://eur-lex.europa.eu/eli/dir/2022/2555/oj

2. PROJECT DESCRIPTION.

2.1 General requirements

The project involves designing and developing IoT objects that comply with the principles of "Secure by Design" and "Green Development". The IoT objects will have to guarantee the security of data and communications, while being environmentally friendly in their design, manufacture and use.

2.2 General

The IoT objects developed must incorporate security features right from the design stage, using secure communication protocols, robust authentication mechanisms and advanced cryptography techniques. They should also be designed to minimise their environmental impact, by promoting energy efficiency, the use of recyclable materials and the reduction of electronic waste.

2.3 Services to be provided by the applicant

The applicant undertakes to work with the service provider to ensure compliance with the principles of "Secure by Design" and "Green Development". This involves providing all the specifications and requirements relating to the security and environmental sustainability of the IoT objects to be developed.
In terms of security, the applicant is responsible for communicating specifications relating to data protection, confidentiality, authentication, integrity and availability of the IoT solution. This includes the definition of security policies, encryption mechanisms, authentication and access management protocols, and security incident management procedures.
Regarding environmental sustainability, the applicant should provide information on requirements for carbon footprint reduction, energy efficiency and responsible use of resources. This may include guidelines on the design of IoT objects to reduce their energy consumption, use sustainable and recyclable materials, and implement efficient energy management mechanisms. The applicant may also specify recycling and waste management criteria to ensure the environmental sustainability of the IoT solution developed.
Collaboration between the requester and the service provider as part of compliance with the principles of "Secure by Design" and "Green Development" is essential to ensure that the IoT solution developed meets the highest security standards and helps protect end users and their data, while minimising its environmental impact.

3. DETAILS OF EQUIPMENT LOCATION

[Indicate here specific details about the location of IoT equipment, for example, whether it will be used in indoor or outdoor environments, or whether it requires specific safety or environmental certifications].

4. TECHNICAL DETAILS OF THE CONTRACT

4.1 Technical specifications

4.1.1 Quality and durability of equipment

The technical description highlights the use of high-quality, environmentally-friendly materials that encourage recycling in IoT objects. This guarantees their durability, reduces the carbon footprint and preserves natural resources, offering high-performance, environmentally-friendly solutions.

4.1.2 Applicable standards and regulations

IoT objects will have to comply with current safety and environmental standards and regulations, conforming to specific directives and certifications.

4.1.3 Site visits

If necessary, a visit to the sites where the IoT objects will be used can be organised to take account of specific safety and environmental constraints.

4.1.4 Knowledge of the site

The service provider must demonstrate its knowledge of the constraints linked to the sites where the IoT objects are used, by identifying the security and environmental aspects to be taken into account in the development of the solutions.

4.1.5 Service limits

The services provided will be limited to the development, deployment and initial configuration of the IoT objects in accordance with the specified requirements. Any subsequent maintenance or upgrades will be subject to a separate agreement.

4.2 Detailed services

4.2.1 Studies

Preliminary studies will be carried out to analyse the security and environmental sustainability requirements of IoT objects, identifying the appropriate technical solutions.

4.2.2 Implementation services

User training: Training for end-users of IoT objects will be provided, focusing on good safety practices and environmentally friendly use measures.

4.2.3 Cleaning and refurbishment

Instructions will be provided for cleaning and refurbishing IoT objects, in compliance with applicable environmental standards.

4.2.4 Guarantees

Guarantees will be provided to ensure the quality, safety and durability of the IoT objects developed.

4.2.5 Supply

The IoT objects developed will be supplied in accordance with the defined technical specifications, ensuring that they comply with the principles of "Secure by Design" and "Green Development".

4.2.6 Tests and checks

Tests and checks will be carried out on the IoT objects to ensure that they comply with the defined security and environmental sustainability standards.

4.2.7 Documentation

Full documentation, including technical specifications, installation and use procedures, as well as safety and maintenance instructions, will be supplied with the IoT objects.

4.3 Scalability

IoT objects must be designed in such a way as to allow them to evolve, with the possibility of adding new functionalities or updating security systems and environmental components.

4.4 Technical support

Technical assistance will be provided to answer questions and problems related to the IoT objects developed, ensuring effective support in terms of security and sustainability.

4.5 Device configuration

The IoT objects will have to be configurable in order to adapt to the specific needs of the applicant, allowing customised configuration while guaranteeing the security and sustainability of the solutions.

4.6 Maintenance contract

If necessary, the terms and conditions of a maintenance contract for IoT objects may be defined separately, specifying responsibilities and maintenance deadlines.

4.7 Technical specifications

The technical specifications will have to include specific requirements in terms of security, data confidentiality, energy efficiency and the use of environmentally-friendly materials.

5. FINAL TERMS

Applicant's signature and stamp: The applicant must sign and stamp his agreement with the terms of the CCTP, thus confirming his willingness to develop secure and environmentally-friendly IoT objects.

6. GENERAL TERMS AND CONDITIONS OF SALE

General terms and conditions, also known as terms and conditions or GTCs, are a set of rules and agreements that govern the relationship between two parties, usually a supplier of goods or services and a consumer. They define the rights, responsibilities and obligations of each party, and cover aspects such as payment terms, delivery times, guarantees, conditions of use of services, dispute resolution and much more. General terms and conditions are often presented as a written document and must be accepted by users or customers before they can benefit from the products or services offered. They play a crucial role in establishing a clear and transparent legal framework, while protecting the interests of both parties involved in a commercial transaction.

7. Appendix

This section contains examples of:

- Cyber-resilience Act
- NIS 2 Act

7.1 Cyber Resilience Act

Summary of the Cyber Resilience Act (15.9.2022): The Cyber Resilience Act aims to guarantee the security of products with digital elements on the European Union market. The text sets out essential requirements for products with digital elements, particularly in terms of vulnerability management and security. Manufacturers must carry out a risk assessment of their products and comply with the applicable security standards.

The text also provides for conformity declaration mechanisms, such as the EU Declaration of Conformity, as well as the use of the CE marking to indicate compliance with the requirements of the regulation. Conformity assessment procedures are defined, which may be carried out by the manufacturer itself or by an independent third party, depending on the level of risk associated with the product.

The importance of coordination and communication between manufacturers, market surveillance authorities, the European Union Cybersecurity Agency (ENISA) and national cybersecurity contact points is emphasised. Manufacturers must notify ENISA of actively exploited vulnerabilities and inform users of security incidents relating to their products.

The text highlights the need to develop harmonised standards and common specifications to facilitate the conformity assessment of products with digital elements. It also provides for cooperation with the European cybersecurity certification framework to facilitate the conformity of certified products.

Finally, the text addresses specific issues relating to certain sectors, such as medical devices, vehicles and high-risk artificial intelligence systems.

7.2 NIS 2

The proposed Directive (EU) 2022/2555 (NIS2) aims to strengthen the security of networks and information systems in the European Union. It aims to ensure a high level of resilience and protection of digital infrastructures, in particular in critical sectors such as energy, transport, health and financial services.

The main provisions of the NIS2 Directive include strengthening governance through cooperation between Member States, extending the scope of application to digital service providers and operators of critical infrastructures, and establishing security obligations to prevent incidents and ensure the resilience of networks and information systems.

The Directive also provides for the notification of significant security incidents to the competent authorities, enabling a coordinated response in the event of an incident, as well as financial penalties in the event of non-compliance with security obligations.

It is important to note that the NIS2 Directive is still under discussion and negotiation. Consequently, the precise details of its provisions may be subject to change before its final adoption.

However, the NIS2 Directive is an essential step towards strengthening digital security in Europe and ensuring the protection of critical infrastructures against cyber threats.