Open Call 1

Guide for applicants

February 2026

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neither the European Union nor the granting authority can be held responsible

Project Title	Resilient and secure Europe: advancing security through green and digital transitions
Project Acronym	CITADEL
Grant Agreement No	101235136
Type of Action	SMP Grants for Financial Support
Topic	SMP-COSME-2024-CLUSTER-01
Start Date of Project	1 October 2025
Duration of Project	36 Months

Dissemination Level	
PU	Public

Version	Date	Document history	Stage	Distribution
V0	08/01/2026	Document drafted	Draft	CITADEL Consortium
V1	03/02/2026	Document review	Draft	CITADEL Consortium, EC
V2	17/02/2026	Document review	Final V2	CITADEL Consortium, EC
V2.1	18/02/2026	Document final	Final V2.1	Public

Table of contents

This project has received funding from the European Union under the Grant Agreement n°101235136.

This project has received funding from the European Union under the Grant Agreement n°101235136.

1. Background on CITADEL project

CITADEL (Project full title: Resilient and secure Europe: advancing security through green and digital transitions) is one of the 16 Euroclusters initiatives, co-funded by the European Commission in the Single Market Programme, under the Grant Agreement number 101235136. CITADEL has been built as a network of 6 European clusters from digital and security sectors :

- SYSTEMATIC Paris-Région (France)
- AKTANTIS (France)
- SAFE (France)
- L3CE (Lithuania)
- ClujIT Cluster (Romania)
- Business Tampere - Safety and Security Cluster (Finland)

CITADEL's goal is to support innovation, networking and adoption of new processes and advanced **technologies on the security value chain.**

The **digital and green transitions** are important drivers in the security sector, offering both challenges and opportunities.

On one hand, the **increasing digitalisation** of critical infrastructures and services introduces new vulnerabilities to cyberattacks and to hybrid threats. On the other hand, digital technologies, such as artificial intelligence (AI) and Internet of Things (IoT), provide powerful tools to improve security measures.

Similarly, the **green transition** raises questions about energy security, resource scarcity and dependencies, and about resilience of renewable energy systems. Moreover, climate change introduces also new security threats, including more frequent natural disasters (wildfires, floods, extreme weather events) that can potentially disrupt critical infrastructures, energy supplies, and public safety.

The overall aims of the CITADEL project are:

- To support stakeholders (and especially companies) in the security ecosystem in adopting advanced technologies that can overall improve the security protection;
- To initiate, develop and maintain a European long-term strategic partnership between companies of different kinds and sizes (with an emphasis on SMEs) in the security value chain and ecosystem;
- To strengthen the security and resilience of critical infrastructures across Europe by fostering innovative solutions that address both physical and digital vulnerabilities;
- To empower SMEs as key innovators, supporting them to foster collaboration, and scale innovative security solutions;
- To use the opportunities presented by digital and green transitions to develop integrated approaches that simultaneously improve security and sustainability;
- To promote strategic collaboration and networking in the security sector by facilitating cross-sectoral and transnational collaboration to address security challenges and create a networked approach to resilience and innovation. CITADEL aims at supporting clusters' activities towards

This project has received funding from the European Union under the Grant Agreement n°101235136.

SMEs to speed up the adoption of digital technologies and processes in the security industrial ecosystem.

On this context, the CITADEL project will focus on fostering innovation, resilience, and sustainability within European security ecosystem by leveraging the synergies between digital and green transitions.

It will support SMEs in developing and deploying advanced security solutions through a cascade funding mechanism, promote cross-sectoral collaboration, and align with EU policy frameworks.

CITADEL seeks gender balance. Therefore, applicants are invited to take all measures to promote equal opportunities between men and women in the implementation of the action. They must aim for a gender balance at all levels of personnel assigned to the action, including supervisory and managerial levels to the extent possible.

2. Basic information about the CITADEL Open Call 1

The CITADEL Open Call 1 is the first call under the CITADEL project.

It will provide financial support to up to 17 innovative projects led by SMEs.

These projects will aim to develop, test, and deploy cutting-edge technologies that enhance the security of territories and infrastructures. Transparent selection criteria will ensure that the most impactful and feasible proposals are funded. Beyond financial support, funded SMEs will receive technical and business mentoring from the CITADEL project partners to maximize the effectiveness and scalability of their solutions.

The CITADEL Open Call 1 will open on 24 February 2026 and close on 5 May 2026, 17:00 CEST.

The total budget for the CITADEL Open Call 1 is 1 020 000 € (60 000 € per project).

A second CITADEL call is expected to be launched in 2027.

3. Scope and expectations

3.1. Type of projects

Financial support will address **demonstration / pilot projects**, targeting companies having already developed a prototype for the security sector and including digital technologies (AI, IoT, Cyber, Photonics), with the need to demonstrate its efficiency on a larger scale, **in a real or near-real environment,** within a testbed, for purpose of innovation uptake and further adoption.

Projects should start at TRL 5-6 (Technology Readiness Level) **and aim to reach TRL 6-7 or higher by the end of the funding**, demonstrating the technology in real or near-real environments to support innovation uptake and adoption.

This project has received funding from the European Union under the Grant Agreement n°101235136.

The financial support will NOT fund the purchase and installation of advanced technologies, but to help accelerate their uptake **by demonstrating, on field and under real (or near-real) conditions the actual feasibility of deployment.**

3.2. Digital technologies

The technological scope of CITADEL focuses on leveraging **advanced digital solutions (IoT, photonics, AI, cybersecurity, and improved communication technologies)** that represent the most promising innovation potential in security market, to enhance security capabilities, enabling smarter monitoring, predictive analytics, threat prevention, and robust emergency response within the security value chain.

The SME projects that will be selected and supported by CITADEL will have to cover at least one of the following technologies (not limitative):

- **Internet of Things (IoT) and Edge technologies** :
  - Smart sensors and sensor networks (environmental, perimeter, structural, chemical, radiological, motion detection)
  - Edge computing and edge AI for real-time data processing and reduced latency
  - Multi-sensor data fusion for situational awareness
  - Embedded systems for autonomous or semi-autonomous monitoring
  - Secure IoT architectures for critical and security-sensitive environments
- **Photonics and optics :**
  - Photonic and optical sensors (LiDAR, infrared, hyperspectral, fiber-optic sensing)
  - Imaging and non-imaging optical systems for detection and surveillance
  - Computer vision systems based on optical and photonic technologies
  - Robotics perception systems (vision, depth sensing, navigation)
  - Advanced optics for low-light, long-range, or harsh-environment monitoring
- **Artificial Intelligence (AI) and data analytics :**
  - AI models for predictive analytics, risk assessment, and decision support
  - Machine learning and deep learning for computer vision and pattern recognition
  - AI-driven anomaly detection and threat identification
  - AI-enabled automation and autonomous systems (including robotics and drones)
  - AI-based digital twins for simulation, testing, and operational optimisation
  - Large-scale data analytics for trend analysis, early warning, and risk prediction
  - Explainable and trustworthy AI for security-critical applications
- **Cybersecurity :**
  - Cyber threat detection, prevention, and incident response systems
  - Security-by-design and privacy-by-design approaches

This project has received funding from the European Union under the Grant Agreement n°101235136.

- Secure data management, encryption, and identity and access management
- Blockchain and distributed ledger technologies for data integrity, traceability, and secure sharing
- Cyber resilience solutions for interconnected and IoT-based security systems

- **Communication, interoperability and response :**
  - Secure communication networks (cloud, edge, hybrid architectures)
  - Interoperable platforms for data exchange across security stakeholders
  - Resilient and redundant communication systems for crisis and emergency situations
  - Real-time information sharing and command-and-control platforms
  - Decision-support and coordination tools for emergency response and crisis management

3.3. Security sector and value chain

The domain and application scope of CITADEL addresses major security challenges by focusing on the protection of critical infrastructures, strengthening resilience to natural and technological hazards, and supporting the safety, sustainability, and resilience of urban environments. These objectives are pursued in alignment with the green and digital transition.

3.3.1. Targeted application domains

Targeted application domains include:

A. **Protection of critical infrastructures**:
   - They are defined as entities/infrastructure providing “essential services” whose disruption would have significant societal/economic impacts. They are characterised by high levels of interconnection, strong interdependencies, regulatory constraints, and increased exposure to physical and cyber threats.
   - The CER Directive (EU) 2022/2557 provides EU sectors/subsectors that are used to identify critical entities.
   - In the scope of CITADEL, they cover the following sectors:
     - Energy
     - Transport
     - Banking and financial market infrastructure
     - Healthcare
     - Water management
     - Digital infrastructure
     - Public administration
     - Space

This project has received funding from the European Union under the Grant Agreement n°101235136.

- Production, processing and distribution of food at large scale

B. **Resilience to natural and/or technological disasters:**

- United Nations Office for Disaster Risk Reduction (UNDRR) defines resilience as the capacity of a system/community/society exposed to hazards to resist, absorb, adapt, and recover while preserving essential functions.
- In the scope of CITADEL, this domain includes climate-related events, industrial accidents, and cascading failures, with a strong link to environmental sustainability and the green transition.

C. **Urban environments (cities, public spaces):**

- Urban security is defined as the overall state in which cities are safeguarded against harm resulting from intentional human actions or behaviours, encompassing both objectively assessed risks and perceived safety, and grounded in evidence-based vulnerability analysis.
- In the scope of CITADEL, this domain addresses security, resilience, and continuity of services in complex and densely populated settings, including the management of large events and crowds to ensure public safety, crowd control, and coordinated emergency response.

3.3.2. Positioning within the security value chain

Proposed projects must position their activities within at least one stage of the security value chain, as outlined below:

1. **Risk assessment and threat identification**

This phase covers the identification and analysis of potential risks and vulnerabilities across physical and digital domains. Typical activities include intelligence gathering, vulnerability assessments, risk mapping, and scenario analysis.

2. **Prevention and mitigation**

Prevention aims to reduce vulnerabilities through organisational, regulatory, and technical measures such as training, policies, and infrastructure reinforcement. Mitigation focuses on limiting the impact of incidents through the deployment of advanced technologies, including AI-based surveillance, cybersecurity solutions, and IoT-enabled monitoring.

3. **Detection and monitoring**

This phase involves the real-time or near-real-time identification of threats and incidents. It relies on advanced technologies such as AI-driven image and signal analysis, IoT sensor networks, and real-time data analytics to detect physical intrusions, abnormal behaviour, or cyberattacks.

4. **Response**

Response activities aim to ensure rapid, coordinated, and effective action following an incident. This includes emergency management, crisis coordination, activation of response services, execution of evacuation or containment plans, and technical countermeasures against cyber or physical threats.

5. **Recovery and business continuity**

This project has received funding from the European Union under the Grant Agreement n°101235136.

Recovery focuses on restoring normal operations and ensuring the continuity of critical services after a disruption. Activities may include post-incident analysis, system recovery and rebuilding, resilience enhancement, and the deployment of improved or upgraded solutions to prevent future incidents.

3.3.3. Security challenges

Annex 1 presents a list of challenges to be addressed that are provided as examples and should not be considered exhaustive. Applicants are encouraged to address other relevant security challenges within the scope of the call.

3.3.4. Expected impacts

Projects are expected to contribute to:

- **Technological innovation**: demonstrate and validate advanced security solutions (AI, IoT, photonics, cybersecurity, communication) at TRL 6-7+, accelerating uptake and deployment
- **Operational and security benefits**: Improve threat detection, resilience of critical infrastructures, emergency response, and safety in urban environments, including crowd and large-event management.
- **Economic and market impact**: Support faster commercialisation, create new business opportunities, and strengthen competitiveness of European security companies
- **Societal and policy impact**: Enhance public trust, support the green and digital transition, and inform security policy and standardisation.
- **Knowledge and learning:** Generate lessons learned, best practices, and insights to guide replication, R&D, and innovation strategies.

4. Consortium composition

Only **collaborative projects, carried out by a consortium of 2 entities**, can be proposed.

The consortium composition must be composed of the following:

	Type of entity	Sector
Partner 1	SME	Digital technologies (offer side)
Partner 2	Private (SME or non-SME) or public entity	End-user, representing the security sector (demand side)

All entities applying as one consortium should be autonomous to one another (without capital or personal links).

This project has received funding from the European Union under the Grant Agreement n°101235136.

The CITADEL partners or their affiliates or employees are NOT considered as eligible applicants and can NOT apply for funding.

Applicants from the EU-13 countries[1] are encouraged to apply.

5. Eligibility conditions

Proposals will be eligible if and only if **all the following conditions** are met:

- Applicants are legal entities located in one of the participating in the Single Market Programme (SMP), namely:
  - EU Member States (including overseas countries and territories (OCTs))
  - non-EU countries: listed European Economic Area EEA countries and countries associated to the COSME (Competitiveness of SMEs) part of the Single Market Programme (list of participating countries as it is as on the opening date of the CITADEL Open Call 1 : https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/smp/guidance/list-3rd-country-participation_smp_en.pdf)
- The consortium composition must comply with the rules described in section 4. The two legal entities that compose the consortium must be independent (no capital link nor no personal link among the two entities).
- At least one of the two legal entities that compose the consortium is a for-profit SME from the digital sector. “For-profit SMEs” means micro-, small- and medium-sized enterprises, as defined in Commission Recommendation 2003/361/EC. Definition here: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en. The SME applicants will need to fill in the self-assessment tool (http://ec.europa.eu/growth/tools-databases/SME-Wizard/) demonstrating their status and include/annex its result into the application platform.
- Applications respect the conditions described in the present guide for applicants; namely the type of action is indicated, the TRL envisaged, the maximum financial contribution per beneficiary and per project and the project maximum duration.
- Applications must be submitted through the dedicated CITADEL platform (https://citadel.grantplatform.com/) before 17:00 CET of the deadline indicated in section 8 of the present guide for applicants.
- Applications must be written in English, in scope and complete in all the parts indicated in application forms; Only parts written in English will be evaluated.
- SMEs that are under liquidation, in difficulty[2], or excluded from the possibility of obtaining EU funding under the provisions of both national and EU law, or by a decision of both national or EU authority are not eligible to apply for funding. Before applying, SMEs will have to check their financial situation by filling out the SME Financial Viability Self-Check. SME applicants must

[1] Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, Slovenia.
[2] According to the Commission Regulation No 651/2014, art. 2.18

This project has received funding from the European Union under the Grant Agreement n°101235136.

provide the outcome of this self-assessment in their application, to prove the SME financial capacity https://ec.europa.eu/research/participants/lfv/lfvSimulation.do.

- Each SME applicant can only be engaged in one application to the CITADEL Open Call. If more than one proposal is submitted by an SME (even with a different entity as partner or for a different project), only the last edited proposal which has been submitted will be evaluated. Other proposals will not be eligible.

The eligibility criteria will be checked based on the information provided in the applications during the whole evaluation process. The applications that do not comply with those criteria will be excluded and marked as ineligible.

By submitting an application, applicants confirm that they have read and accept the terms and conditions outlined in this Guide for Applicants.

6. Funding conditions

Only for-profit SMEs are eligible to receive funding.

The **maximum funding per project is 60 000 €,** for a duration of **maximum 9 months**.

This financial support to each selected project will have to represent a **maximum of 80% of the funded project's budget**, resulting in a co-financing based on **private financial resources of at least 20%.**

Applicants must submit a project budget at the application stage, showing a **total project cost of at least 75 000 €**, with a requested CITADEL contribution of 60 000 € (lump sum) and a minimum private financial contribution of 15 000 €.

It will be up to the applicants to declare which type of private financial sources they will use (debt or own financial sources) for their project, and to confirm this amount into the final report of their project, if selected for funding. Crowding-in of private resources means financial resources invested in the project, i.e. not as in-kind contributions, staff costs or similar.

For consortia composed of two SMEs, the total **CITADEL contribution of 60 000 € can be shared** between them. The financial split is decided by the SMEs, but any SME requesting funding must receive at least 10 000 €.

The funding will be provided under the form of a **lump sum:**

A lump sum is a fixed amount of money which can be used by beneficiaries for several purposes related to the achievement of the project objectives. It is necessary to provide an explanation in the application on how the lump sum will be used (personnel costs, subcontracting, travels, equipment) but detailed reporting of the spending, cost statements and time sheets are not requested after the end of the project, unless in case of audits. Since the granting of a lump sum does not foresee the delivering of a cost statement, the use of the project budget will be controlled considering the technical advancements by the technical reviewers.

Subcontracting costs are allowed but not exceeding 30% of each SME budget.

The final technical evaluation will assess the coherence of the spent money with the achieved results.

This project has received funding from the European Union under the Grant Agreement n°101235136.

7. Application process

Guide for applicants can be downloaded from the following link: https://citadel.grantplatform.com/

Applications must be submitted through an online tool built on the Goodgrant platform, specifically designed for the publication, management, and evaluation of CITADEL Open Call 1.

The application platform can be accessed at: https://citadel.grantplatform.com/ . It provides the call front page with all relevant information, guidelines, and application conditions.

All applications for CITADEL Open Call 1 must be submitted exclusively via this platform.

Applicants must first create an account on the aforementioned website. After registration, a dedicated application form will be made available, in which all required information must be entered using text fields, drop-down menus, or similar input formats. Applicants are also required to upload additional documents in PDF format (e.g. letter of support, if applicable; results of the self-financial viability check; results of the SME self-assessment).

Applicants may start an application, save it as a draft, and return to complete or modify it as many times as necessary prior to final submission. Draft applications can be accessed at any time until the submission is completed, and the call deadline is reached.

The last step in the application process is clicking the final submission button. Once applicants have finally submitted their proposal, they receive an automated e-mail stating that the submission has been entered successfully.

Applicants are strongly encouraged to complete the application form with the utmost care and accuracy, as the information provided therein will be binding and, in the event of selection, will form an integral part of the sub-grant agreement.

8. Timeline

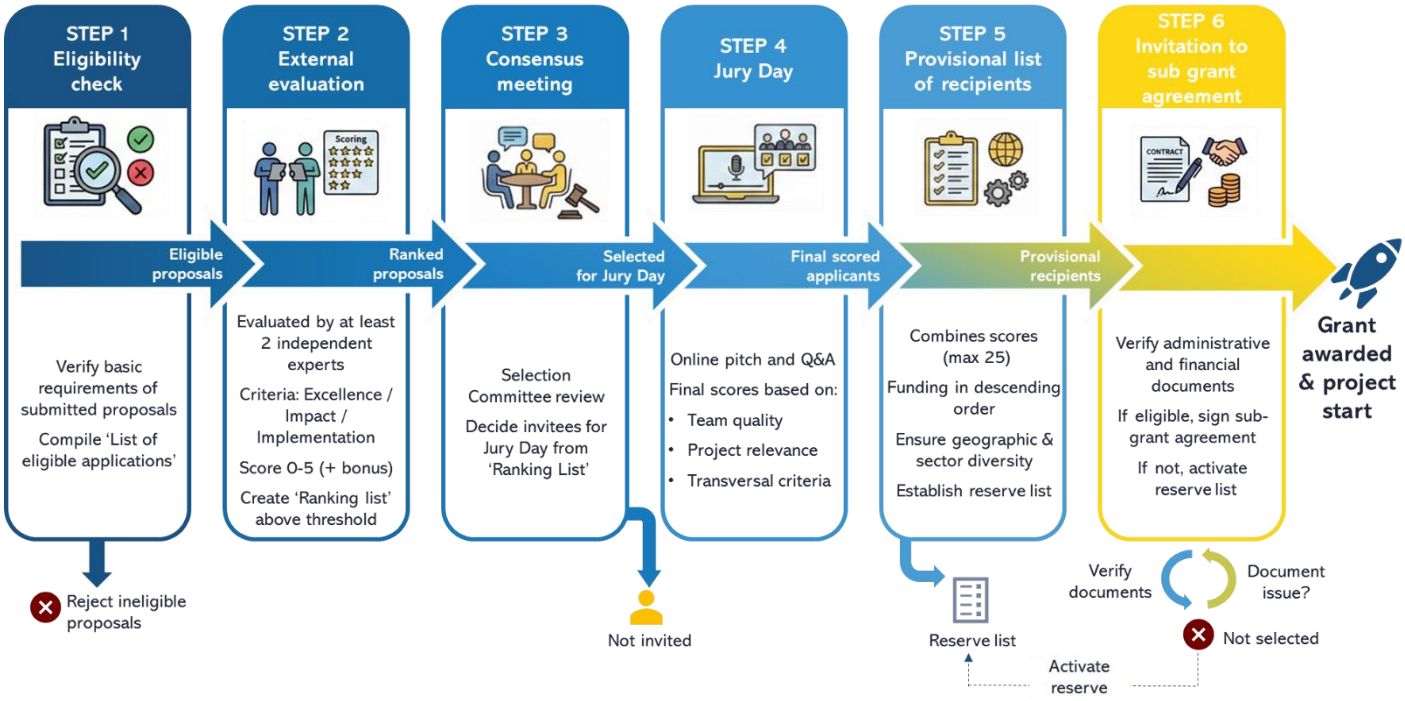
- **24 February 2026: Opening of the call**
- **05 May 2026: Deadline of the call at 17:00 CEST**
- 05 May 2026 – 10 May 2026: Eligibility assessment (administrative check)
- 11 May 2026 – 26 May 2026: Evaluation by external experts
- 01 June 2026 : Information to shortlisted applications invited to Jury Day
- **15 – 16 – 17 June 2026: Online jury day (pitching auditions)**
- 18 June 2026 : Information to selected applicants, with request of administrative documents
- 01 July 2026 – 11 September 2026: Sub-grant Agreement signature for the selected applicants
- **01 October 2026 – 30 June 2027 : Execution/implementation of selected projects**
- **September 2027 : Presentation of the projects' results during a dedicated workshop**

In the event of being shortlisted, applicants must ensure they reserve the jury day in their calendar. The date is fixed, and online attendance is mandatory to present the pitch for the shortlisted projects.

This project has received funding from the European Union under the Grant Agreement n°101235136.

9. Evaluation and selection process

Submitted proposals will be evaluated in multiple phases, as outlined in the figure below.



9.1. Step 1 : First eligibility check

The first evaluation step focuses on verifying the basic requirements based on the information from the submitted proposals, as indicated in section 5. The submitted proposals will be admissible for the next phase if it:

- It is complete, readable and in English in all mandatory sections.
- It has been submitted via the online form https://citadel.grantplatform.com/ within the deadline (cf section 7).
- The consortium composition complies with the requirements of section 4.
- It includes the properly filled declaration of honour, and attached documents (SME declaration, SME financial viability check).

Proposals that do not meet these criteria will be rejected. After this verification, a "List of Eligible Applications" will be compiled.

9.2. Step 2 : External evaluation

In this phase, each eligible proposal within the 'List of Eligible Applications' will be evaluated by at least two external and independent evaluators, appointed according to the specific characteristics of the applications from the pool of External Experts. This pool will be composed of external evaluators who

This project has received funding from the European Union under the Grant Agreement n°101235136.

respond to a Call for Expression of Interest for Evaluators, which will be launched with the aim of selecting the most suitable independent experts.

The external evaluators will receive evaluation guidelines and templates and will be duly informed about the timing to ensure a swift and efficient process. All appointed external evaluators will sign a declaration of no conflicts of interest and a non-disclosure agreement.

The evaluation will be done according to the following criteria (same weights for the three criteria):

1. **Excellence:**
    - Soundness and pertinence of objectives with the scope of the call
    - Credibility of the technological KPIs to measure the results
    - Concreteness of the technical approach
    - Coherence of the TRLs
    - Innovativeness of the proposed solution
2. **Impact:**
    - Industrial and market relevance: alignment of the project with key security challenges, relevance for the security sector including potential for adoption by end-users
    - Contribution to strengthening competitiveness and innovation capacity of European companies in the security market
    - Environmental and societal dimension:
        - Contribution to the green and digital transition (energy-efficient, sustainable, low-carbon solutions)
        - Positive societal impact, such as enhancing public safety, protecting citizens, or improving urban resilience
        - Attention to ethical, privacy, and social responsibility aspects, particularly for AI, IoT, or surveillance technologies
    - Quality of the exploitation, market opportunity, IPR (Intellectual property rights) and knowledge protection strategy
3. **Implementation**
    - Soundness of the workplan, including relevance of the tasks described, and the timing of the activities
    - Risk assessment and mitigation strategy: Identification of technical/operational risks and adequacy of proposed mitigation measures
    - Appropriateness of the consortium: evaluate completeness (digital Technology providers and security end-users are present) and complementarity (the provided solutions match with the needs of the final users), expertise of the team
    - European dimension (in terms of transnational dimension of the consortium and exploitation intentions towards European countries)
    - Cost-effectiveness of the workplan and budget: quality and effectiveness of the resources assigned to the project in order to get the proposed objectives/deliverables

This project has received funding from the European Union under the Grant Agreement n°101235136.

- Operational capacity (evaluate the technical capacity of the applicants/consortium related to the proposed work)

A score from 0 to 5 including half scores will be assigned to each of the 3 criteria.

The meaning of score marks is as follows:

- 0 - The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
- 1 - Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.
- 2 - Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.
- 3 - Good. The proposal addresses the criterion well, but a number of shortcomings are present.
- 4 - Very Good. The proposal addresses the criterion very well, but a small number of shortcomings are present.
- 5 - Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

For each application above the threshold, applications in which the 2 participating entities are from 2 different countries (transnational bonus point) will be given one bonus point.

The final score will be calculated as an average of the individual assessments provided by the evaluators, plus up to the bonus point if applicable.

The **threshold** for each individual criterion is 3 out of 5 points. The overall threshold, which applies to the sum of the four individual scores, is 10 out of 15 points. The maximum total score is 16 points (including the bonus point).

In the case of ties, the following criteria will be used to rank the projects, in order: 1) Impact score, 2) Implementation score, 3) Excellence score. In case of further tie, priority will be given to projects with partners coming from EU-13 countries[3].

A 'Ranking List' will be created and all applications that score above the threshold will proceed to the next step.

9.3. Step 3 : Consensus meeting

Based on the 'Ranking List', the 'Selection Committee' (composed of one representative of each CITADEL project's partner) will decide, at this stage, the 'List of Jury Day's participants' to be invited to the Jury Day.

Maximum number of applicants to be invited to the Jury Day is 24.

[3] Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, Slovenia.

This project has received funding from the European Union under the Grant Agreement n°101235136.

9.4. Step 4 : Jury day (auditions)

Shortlisted applicants will be invited to an **online** Jury Day that is foreseen on **15 – 16 – 17 June 2026**.

Participation of at least one consortium member from the shortlisted applicants will be mandatory. It is recommended that both consortium members are present at the Jury Day.

During the Jury Day, applicants will have the opportunity to pitch their project in front of the CITADEL Jury composed of the CITADEL Selection Committee Members. The Selection Committee could be supported by security and digital experts. The pitch will be followed by a Q/A session with the Jury.

The CITADEL Selection Committee will undertake the evaluation with the following criteria:

1. Quality of the team
2. Matching with CITADEL objectives, including :
    a. Innovative step in solving security issues
    b. Feasibility of the project implementation
3. Transversal criteria (environmental impact, low carbon, equal opportunities).

For criteria 1 and 2 : A score from 0 to 4 including half scores will be assigned

For criteria 3 : A score from 0 to 1 including half score will be assigned

Maximum score of the Jury Day is 9 points.

The final scores for the jury day of each application will be calculated as an average of the individual assessments provided by each member of the CITADEL Jury.

9.5. Step 5 : Provisional list of FSTP recipients

The CITADEL Selection Committee will prepare a final ranking list **by combining the scores from two phases: the external evaluation** (including a bonus point for transnational consortia, maximum 16 points) **and the CITADEL Jury Day** (maximum 9 points). **The highest possible total score is 25 points.**

Successful proposals are funded in descending order until the available budget for the call is totally assigned. The CITADEL Selection Committee composed of one representative of each CITADEL project's partner reserves the right of modifying the ranking of successful proposals (in case of equal scores) in order to balance the list of selected projects according to geographical coverage and security sectors represented, to better reflect diversity of sectors and countries covered in Europe.

At least 10% of the supported SMEs will be based in EU regions other than those of the individual CITADEL partners, specifically outside Finland, France, Lithuania, and Romania.

An Evaluation Summary Report containing the scores and Evaluators' justifications for each score as well as the Selection Committee ranking justifications will be provided to the applicants.

Following the evaluation process, a reserve list may be established. Applications placed on the reserve list may be invited for funding in the event that selected projects withdraw or fail to meet contractual requirements

This project has received funding from the European Union under the Grant Agreement n°101235136.

9.6. Step 6 : Invitation to Sub grant agreement preparation and signature

Participating entities from the successful applications selected for funding will firstly have to provide a number of administrative and financial documents to confirm their eligibility. Applicants will have a maximum delay of two weeks to provide the requested documentation.

The CITADEL Consortium will proceed to a verification of these documents to make sure the selected applications are eligible.

Selected applicants at the stage are requested to be extremely cautious regarding:

- **The nature of the documents requested:** If the documents that are provided do not prove the eligibility, the participation of concerned applicants will be terminated at this stage.
- **The deadlines for document submission:** If the requested documents are not submitted on time, and without a clear and reasonable justification, the applicant will be excluded from further formal check. In this case, another applicant from the 'Reserve List' will be selected.

If all eligibility conditions are indeed met and confirmed, participating entities from the successful applications selected for funding will be invited to sign a sub-grant agreement with SYSTEMATIC Paris-Région, coordinator of the CITADEL project. This sub-grant agreement contains the obligations of the SMEs funded in the framework of CITADEL Open Call (including conflict of interest, confidentiality and security, ethics, visibility, information and record-keeping) and payment process to be proceeded by the CITADEL Coordinator.

Applicants that are invited to prepare and sign a sub-grant agreement should note that the content of their submitted application, as approved during the evaluation process, will constitute an integral and binding part of the sub-grant agreement.

10. Support from CITADEL, reporting and payment arrangements

10.1. Monitoring and reporting

Each funded project within the CITADEL Open Call 1 will be followed and monitored by one CITADEL consortium partner. The assigned CITADEL consortium partner will be in charge of following and assessing the progress of the funded projects.

Specific template will be provided by CITADEL to the funded projects for the mid-term reporting and the final reporting. These templates will include a dedicated survey addressed to SMEs.

The projects' performance will be assessed:

- During interim review at mid-term, based on a mid-term report provided by the funded projects
- During the final review at the closure of the funded projects, based on the final report provided by the funded projects

This project has received funding from the European Union under the Grant Agreement n°101235136.

A physical or remote meeting with an interactive session will be organised to better verify the quality of the technical results.

The final payment will be done once the final report is approved by the CITADEL consortium partners, based on the following criteria:

- Deliverables quality and completeness (including demonstrators)
- Technical performance indicators (based on the KPIs established in the applications).
- Deadline Compliance.

Should the technical check be unsatisfactory, CITADEL Steering Committee can decide to revoke the funding in whole or in part.

Additionally, at the final stage, beneficiaries will be required to participate in an online public event to showcase their project. Participation to this online event foreseen in September 2027 will be mandatory.

10.2. Payment arrangements

Successful applications shall receive the requested financial contribution in the form of a lump sum according to the following timeline:

- **Pre-financing (up to 20%):** A pre-financing payment of up to 20% of the requested financial contribution (i.e. up to 12 000 €) may be provided at the beginning of the project. The pre-financing is subject to prior approval and risk assessment. Depending on the financial capacity, risk profile, or other relevant considerations related to the beneficiary, the CITADEL consortium reserves the right not to grant any pre-financing.
- **Final payment (up to 80% or up to 100%):**
  - In case pre-financing is granted, the remaining balance of up to 80% of the requested contribution (i.e. up to 48 000 €) will be paid after approval of the final report.
  - In case no pre-financing is granted, up to 100% of the requested financial contribution may be paid upon approval of the final report.

10.3. Promotion of the action of visibility to EU funding

Funded applicants are expected to promote their project, the CITADEL initiative, and its results to relevant audiences, including the media and public, while acknowledging EU funding. The CITADEL consortium will support and guide these activities.

Unless otherwise agreed with the European Commission or CITADEL coordinator, all communication and publicity, including social media, events, presentations, brochures, equipment, and results, must:

- Display the EU emblem and “"Co-funded by the European Union” logo
- Display the CITADEL logo
- Euroclusters logo

Include the statement: “Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European

This project has received funding from the European Union under the Grant Agreement n°101235136.

Innovation Council and SMEs Executive Agency (EISMEA). Neither the European Union nor the granting authority can be held responsible for them."

The EU emblem must be clearly visible and its use does not give exclusive rights. Beneficiaries do not need prior EC permission to use it.

All communication must also clarify that it reflects only the author's views, and that the European Commission and CITADEL project are not responsible for any use of the information.

10.4. Monitoring, audits and compliance

The European Commission (EC) will monitor that CITADEL beneficiaries, including SMEs, comply with the grant agreement and conditions for financial support. The EC may carry out financial audits or on-the-spot inspections during the project and up to five years after its completion, either through EC services, external auditors, European Anti-Fraud Office (OLAF), European Public Prosecutor's Office (EPPO) or European Court of Auditors (ECA). Audits may cover finances, management, and compliance with the grant agreement.

Beneficiary SMEs must provide all requested information and data, including accounting and personnel details, and keep all project documents and deliverables (originals or authenticated copies, including electronic) for five years after project completion.

In case of audits, SMEs must ensure auditors have on-site access to offices, systems, and records and that data is readily available or handed over in an appropriate format.

Based on audit findings, the EC may take appropriate measures, including recovery of payments or other sanctions. The European Court of Auditors may also carry out checks with the same rights as the EC.

11. Helpdesk and FAQ

11.1. Contacts and FAQ

A helpdesk is provided via the email address citadel@aktantis.com

A FAQ document will also be available here: https://citadel.grantplatform.com

The template of the application form (**for information only** – all fields must be directly entered into the application platform https://citadel.grantplatform.com/) is also available on the application platform.

11.2. Complaints

If, after receiving the results of the evaluation phase, an applicant considers that a mistake has been made, resulting in the rejection of the application, a complaint can be sent (in English and by email) to citadel@aktantis.com within five working days following the official receipt of the Evaluation report, including the following information.

- contact details and name of the application

This project has received funding from the European Union under the Grant Agreement n°101235136.

- subject of the complaint
- information and evidence regarding the alleged mistake

The CITADEL consortium will review it within no more than 10 calendar days from its reception. If the CITADEL consortium needs more time to assess the received complaint, the applicant will be informed by email about the extension.

Most of the evaluation process is run by independent external experts in the given field. The CITADEL project consortium does not interfere with their assessment; therefore we will not evaluate complaints related to the results of the evaluation other than related to the mistakes in the evaluation of the eligibility criteria.

12. Confidentiality and GDPR Data protection

12.1. Application stage

A full list of applicants will be prepared containing their basic information for statistical purposes and clarity, which will be also shared with the European Commission for transparency. The applicants' list will not be public but will serve as statistics in project communication materials.

12.2. Evaluation stage

To process and evaluate proposals, the CITADEL consortium will need to collect personal and corporate data. AKTANTIS (Pôle SCS) will act as a Data Controller for data submitted through the Goodgrants platform for CITADEL Open Call 1. The Goodgrants platform's system design and operational procedures ensure that data are managed in compliance with The General Data Protection Regulation (EU) 2016/679 (GDPR). Each applicant will accept the Goodgrants terms to ensure coverage.

CITADEL may share the proposals with selected external independent evaluators, with whom Non-Disclosure Agreements are signed to protect the confidential information given by the applicants.

The final list of the awarded projects and SME applicants/beneficiaries will be made public, including name of the projects, abstract, legal name of the companies, sector, country/region of origins, results of the project, duration of the projects, project budget and date of the award.

This project has received funding from the European Union under the Grant Agreement n°101235136.

Annex 1 – List of challenges

This list presents challenges that are provided as examples and should not be considered exhaustive. Applicants are encouraged to address other relevant security challenges within the scope of the call.

Domain	Security value chain	Challenges
A. Critical infrastructures (CI)	**1. Risk assessment**	- CI practitioners need to have practical, comparable methodology "toolbox" to rank risks (incl. cyber), repeatable risk-analysis procedures aligned to EU expectations for critical entities/operators for compliance. - Models and tools should be able to anticipate cascading consequences, reflect functional/operational consequences. - Models and tools should provide wide risk picture that includes cross-infrastructure dependencies and cascading effect. - Dynamic models needed to assess complex "system-of-systems" environments and support ongoing vulnerability identification and tracking. - Models and tools should include CPS (Cyber-Physical-Systems) elements.
	2. Prevention	- Prevention of decentralised and complex infrastructures requires to expand the cyber surface in monitoring/control layers, so mitigation requires hybrid security models and operational countermeasures. - Models and tools needed for auditable logging of access/usage activities, device access control and verification. - Solutions and tools to confront legacy security gaps. - For effective mitigation planning realistic, sector specific, cyber-range type and scenario-based training simulations to test prevention plans, alerting concepts etc. are needed. - Models and tools for environmental risk assessment.

This project has received funding from the European Union under the Grant Agreement n°101235136.

	3. Detection	- Anomaly detection and monitoring solutions able to fuse heterogeneous signals, support multi-layer and multi-device monitoring. - Methods and tools for recognition of manipulated data/information flow (anomaly detectors can be manipulated by adversarial techniques). - Models and tools providing interpretability and root-cause support and indicating cascading effects to distinguish cyber, physical, and combined anomalies. - Methods and tools for false-alarm reduction. - Distributed/federated detection architectures are needed so monitoring can be effective without centralising sensitive data.
	4. Response	- Decision support models and tools, that justify interdependencies and cyber-physical consequences, provides interpretable situational awareness across different stakeholders. - Methods and tools for rehearsed incident response plans and “survivable” backup/restore practices. - Virtual decision-support environments to predict evolving system states and impacts, fast enough, to support operational response. - Methods and tools for rehearsed incident response plans and “survivable” backup/restore practices. - Methods and tools capable to propose a selection of recovery actions under attack.
	5. Recovery	- Solutions, as digital twin, for simulations and predictive analytics enabling fast control and recovery strategy selection. - Methods and tools enabling swift prioritization, identifying high-impact nodes, rerouting, “accessibility-first” recovery actions, reassign and similar actions. - Supplementary communication channels when operator communications are disrupted, in some cases Global Navigation Satellite System (GNSS) -independent. - Methodologies, procedures and tools for pre-planned restoration logistics, merging data accrued during downtime. - Ensuring power continuity.

This project has received funding from the European Union under the Grant Agreement n°101235136.

B. Resilience	**1. Risk assessment**	- Scenario-based loss estimation to test "what-if" interventions (e.g., retrofitting options) and to plan emergency scenarios using risk assessment outputs. - Near real-time impact modelling that combines hazard magnitude, exposed populations/assets, and vulnerability factors, producing early consequence estimates for decision-making. - Integrated reporting that goes beyond "risk scores" to include actionable context (e.g., affected areas, expected damage, logistics constraints, nearby critical infrastructure, potential secondary effects, and forecasts). - Risk models need to exploit open/public domain data and web-based delivery, because global/large-area consequence analysis at speed depends on accessible data sources and scalable dissemination. - Reproducible and transferable risk assessment frameworks (open tools, reusable workflows) so they can be adoptable.
	2. Prevention	- Prevention/mitigation methods and tools for urban hazards (e.g.: flooding) needs an integrated "full hazard risk management cycle" and not single-measure fixes, because impacts are compound (infrastructure damage, business interruption, community disruption). - Mitigation measures must integrate human factors (e.g., passenger behaviour under blast/terror conditions) into system design. - Operators need design changes to "critical systems" that improve survivability and post-incident operability, so response actions (evacuation, rescue, isolation) remain possible after damage. - Communication approaches are needed that motivate protective actions by households and organisations, otherwise planned measures might underperform. - Climate-scenario-aware planning (e.g., under different RCP trajectories) to size and prioritise mitigation investments now, rather than relying on historic climate baselines.
	3. Detection	- Multi-hazard early warning requires tools with integrated AI that combines meteorological and geospatial modelling for impact prediction. - Intuitive interfaces and feedback loops (user-centric design) so early-warning outputs support real decision-making. - Operators need an interpretable (e.g., in health sector) metric plus a usable dashboard/visualisation layer, because raw anomaly scores and alert floods do not translate into actionable situational awareness. - Reliable detection and classification of drone threats. - A green-transition-relevant need is extending monitoring from "immediate warning" to longer horizons (e.g., ensemble-informed outlooks) so authorities can plan proactive adaptation investments.

This project has received funding from the European Union under the Grant Agreement n°101235136.

	4. Response	- Recourse management systems, that partially automate evacuation or similar activities. - Emergency response planners need co-resilience metrics and visual mapping tools that identify how failures (e.g.: power grid) cascade into other disruptions (e.g.: roadway/transit network), because response resources cannot be effectively allocated without understanding which segments lose accessibility when upstream infrastructure fails. - Cross-boarder and cross-institutional data sharing and collaboration capabilities during evacuations or similar events. - Pre-established crisis communication innovative solutions that function under extreme conditions. - Event advanced early warning systems are ineffective if messages are not clear, timely, and framed so end-users can evaluate options and act.
	5. Recovery	- Recovery needs to be planned as a long-term, multi-sector programme (not an ad hoc “rebuild”), including explicit priorities for infrastructure restoration, public health impacts, and community resilience over months/years. - Recovery models that account for "recovery propagation" dynamics – where restoration of one node enables restoration of dependent nodes – because static repair sequencing fails to capture how cascading failures reverse during the recovery phase. - Continuity planning should include an inventory of technologies that shape “soft/hard” adaptation limits and incorporate disaggregated reporting, so investments can be targeted where recovery capability is structurally constrained. - Recovery governance needs reporting/accountability mechanisms for loss-and-damage and technology effectiveness (what tools were available, used, and whether they reduced impacts). - Capacity building are continuity enablers: without sustained funding/training, systems revert to minimal/copycat solutions and recovery performance stagnates

This project has received funding from the European Union under the Grant Agreement n°101235136.

C. Urban environment	**1. Risk assessment**	- Systemic (e.g., network-level) risk assessment that covers the full chain from regional hazard → component fragility → functionality loss → socio-economic impacts, rather than asset-by-asset assessments. - Context segmentation is needed: Crime Prevention Through Environmental Design (CPTED) -relevant risk factors differ by space type (parks vs other spaces), built form (old vs modern parks), and user groups; assessments must stratify rather than apply uniform scoring. - Governance is part of the risk picture: planning/security assessments must account for multi-actor responsibilities and rights/access trade-offs, otherwise risks persist due to implementation gaps and discriminatory dynamics. - Risk baselining is methodologically hard: inconsistent measures and heterogeneity (across sites and studies) limit comparability, weakening prioritisation and business-case justification. - Consideration of operational strain during blackouts, complicating emergency response.
	2. Prevention	- Multi-actor coordination (planning, safety, owners/operators) is required; fragmentation delays implementation and weakens sustainability. - Prevention-by-design must balance security with openness, accessibility, and livability; over-hardening reduces acceptance and use. - Modeling and optimizing cascading power outages affecting the cities. - Evidence/comparability gap: cities lack consistent evaluation baselines and indicators, so “what works” is hard to compare across sites. - Crime Prevention Through Environmental Design (CPTED) effects vary by site type and user group, so users need segmentation guidance rather than one-size-fits-all design rules.

This project has received funding from the European Union under the Grant Agreement n°101235136.

	3. Detection	- Operational accuracy constraints: dense crowds, occlusion, and varying viewpoints/lighting drive missed detections and false alarms; monitoring solutions must be validated under these real public-space conditions. - Systems must reduce operator overload and provide outputs that can be quickly validated by humans, not just opaque alerts. - Separating physical surveillance from cyber monitoring creates blind spots; users need fused cyber–physical anomaly correlation for realistic hybrid-incident detection. - Real-world monitoring and dataset creation require privacy-by-design, lawful/ethical data capture, and mechanisms that respect participant/user agency. - Drone and other flying objects detection.
	4. Response	- Logistical and coordination challenges under concurrent natural, cyber, and security pressures. - Response needs integrated, real-time fusion/visualisation of heterogeneous streams (GIS + sensors + video + calls/social data). - Rapid spread of misinformation and disinformation, causing unwanted public behavior during crisis events. - Responders often lack building-level semantic/architectural information and indoor routing certainty; response benefits from integrated indoor–outdoor 3D models / digital-twin style views to support navigation and planning. - Digital systems used during response vary widely by locality; challenges recur around reliability, hardware, usability, and interoperability with dispatch centres, hospitals, and other third parties.

This project has received funding from the European Union under the Grant Agreement n°101235136.

	5. Recovery	- A unified, decision-grade “digital backup” of city assets and dependencies (geospatial + utilities + transport + buildings + population); without it, restoration choices are slower and less evidence-driven. - Continuity of essential services requires PPP-style governance, legal/organisational frameworks, and shared monitoring/evaluation mechanisms. - Interoperability constraint: recovery/continuity requires integrating heterogeneous monitoring and assessment data (including cascading effects) into a single operational environment with multidimensional indicators. - Digital-service restoration adds a cross-operator challenge: post-disaster recovery of cloud/telecom services often requires datacentre–carrier cooperation, but information-sharing constraints can delay restoration and complicate prioritization. - Data quality/verification is a practical bottleneck for reconstruction planning; post-event spatial data pipelines (e.g., OSM/remote sensing) require validation procedures to be decision-grade.

This project has received funding from the European Union under the Grant Agreement n°101235136.