



Digital Europe Programme (DIGITAL)

Call for proposals

Accelerating best use of technologies
(DIGITAL-2022-DEPLOY-02)

Version 1.0
15 February 2022



HISTORY OF CHANGES			
Version	Publication Date	Change	Page
1.0	15.02.2022	▪ Initial version (new MFF).	
		▪	
		▪	
		▪	



EUROPEAN HEALTH AND DIGITAL EXECUTIVE AGENCY (HaDEA)

HaDEA.B - Digital, Industry and Space
HaDEA.B.2.01 – Digital Europe

CALL FOR PROPOSALS

TABLE OF CONTENTS

0. Introduction	5
1. Background.....	6
2. Objectives — Scope — Outcomes and deliverables — KPIs to measure outcomes and deliverables — Targeted stakeholders — Type of action — specific topic conditions.....	8
DIGITAL-2022-DEPLOY-02-EBSI-SERVICES – EBSI - Deployment of services	8
Objectives	8
Scope.....	9
Outcomes and deliverables	11
KPIs to measure outcomes and deliverables.....	12
Targeted stakeholders	12
Type of action	12
Specific topic conditions.....	12
DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD – Blockchain Standardisation	13
Objectives	13
Scope.....	13
Outcomes and deliverables	14
KPIs to measure outcomes and deliverables.....	14
Targeted stakeholders	15
Type of action	15
Specific topic conditions.....	15
DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID - Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation	16
Objectives	16
Scope.....	16
Outcomes and deliverables	17
KPIs to measure outcomes and deliverables.....	18
Targeted stakeholders	18
Type of action	19
Specific topic conditions.....	19
DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI - Security (law enforcement): AI-based pilots	19
Objectives	19

Scope.....	20
Outcomes and deliverables	21
KPIs to measure outcomes and deliverables.....	22
Targeted stakeholders	22
Type of action	23
Specific topic conditions.....	23
3. Available budget.....	23
4. Timetable and deadlines	24
5. Admissibility and documents	24
6. Eligibility.....	25
Eligible participants (eligible countries).....	25
Consortium composition	26
Eligible activities.....	26
Ethics.....	27
Security.....	27
7. Financial and operational capacity and exclusion.....	28
Financial capacity	28
Operational capacity	29
Exclusion	29
8. Evaluation and award procedure	30
9. Award criteria.....	31
10. Legal and financial set-up of the Grant Agreements.....	32
Starting date and project duration	32
Milestones and deliverables.....	33
Form of grant, funding rate and maximum grant amount.....	35
Budget categories and cost eligibility rules.....	35
Reporting and payment arrangements.....	36
Prefinancing guarantees	37
Certificates	37
Liability regime for recoveries	37
Provisions concerning the project implementation.....	38
Other specificities	38
Non-compliance and breach of contract	38
11. How to submit an application.....	39
12. Help	40
13. Important	41
Annex 1	44
Annex 2	47

0. Introduction

This is a call for proposals for EU **action grants** in the field of Accelerating best use of technologies under the **Digital Europe Programme (DIGITAL)**.

The regulatory framework for this EU Funding Programme is set out in:

- Regulation 2018/1046 ([EU Financial Regulation](#))
- The basic act (Digital Europe Regulation 2021/694¹).

The call is launched in accordance with the [2021-2022] Work Programme² and will be managed by the **European Health and Digital Executive Agency (HaDEA)** ('Agency').

The call covers the following **topics**:

- **DIGITAL-2022-DEPLOY-02-EBSI-SERVICES** – EBSI – Deployment of services
- **DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD** – Blockchain Standardisation
- **DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID** – Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation
- **DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI** – Security (law enforcement): AI-based pilots

Each project application under the call must address only one of these topics. Applicants wishing to apply for more than one topic, must submit a separate proposal under each topic.

We invite you to read the **call documentation** carefully, and in particular this Call Document, the Model Grant Agreement, the [EU Funding & Tenders Portal Online Manual](#) and the [EU Grants AGA – Annotated Grant Agreement](#).

These documents provide clarifications and answers to questions you may have when preparing your application:

- the [Call Document](#) outlines the:
 - background, objectives, scope, activities that can be funded and the expected results (sections 1 and 2)
 - timetable and available budget (sections 3 and 4)
 - admissibility and eligibility conditions (including mandatory documents; sections 5 and 6)
 - criteria for financial and operational capacity and exclusion (section 7)
 - evaluation and award procedure (section 8)

¹ Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme (OJ L 166, 11.05.2021).

² Commission Implementing Decision C/2021/7914 of 10.11.2021 concerning the adoption of the multiannual work programme for 2021 - 2022 and the financing decision for the implementation of the Digital Europe Programme.

- award criteria (section 9)
- legal and financial set-up of the Grant Agreements (section 10)
- how to submit an application (section 11).
- the Online Manual outlines the:
 - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')
 - recommendations for the preparation of the application.
- the AGA — Annotated Grant Agreement contains:
 - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant (*including cost eligibility, payment schedule, accessory obligations, etc*).

1. Background

The Digital Europe Programme will reinforce EU critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, governance and processing, the deployment of these technologies and their best use for critical sectors like energy, climate change and environment, manufacturing, agriculture and health.

The Digital Europe Programme is strategic in supporting the digital transformation of the EU industrial ecosystems. It targets upskilling to provide a workforce for these advanced digital technologies. It also supports private sector, small and medium-sized enterprises (SMEs), and public administration in their digital transformation with a reinforced network of European Digital Innovation Hubs (EDIH). The Digital Europe Programme will accelerate the economic recovery and drive the digital transformation of Europe.

During 2021-2022, one of the priorities of the Digital Europe Programme is 'accelerating best use of technologies'. Under 'accelerating best use of technologies', the roll-out and best use of digital capacities will focus on priority areas such as the support to the Green Deal, to SMEs and public authorities in their digital transformation and will also provide resources to those activities started in previous programmes, for which the continuations of funding is essential not to disrupt the services provided.

This call will cover EBSI - Deployment of services, Blockchain Standardisation, Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation and Security (law enforcement): AI-based pilots as call topics that fall under the Accelerating Best Use of Technologies priority.

1. **EBSI - Deployment of services and Blockchain Standardisation** - The European Blockchain Services Infrastructure (EBSI) is the first EU-wide blockchain infrastructure driven by the public sector, addressing cross border services in full respect of European values and regulations. EBSI relies on a network of distributed nodes set-up across Europe. This infrastructure aims at leveraging blockchain technology to implement cross-border services for the benefit for citizens, society, and the economy. EBSI is publicly driven and aims to improve on-line services to or interactions between citizens, organizations and public authorities. It can also support cooperation with private actors. In doing so EBSI aims to accelerate the uptake of blockchain in Europe, in

connection with other technologies and other blockchain initiatives, building capacities to reinforce the European blockchain ecosystem.

2. **Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation** - The call aims to facilitate the implementation of the European Digital Identity framework following the proposal for a European Digital Identity Framework³ and the Recommendation for a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework (Toolbox Recommendation)⁴. The broader objective of the European Digital Identity Framework is to improve citizen's access to highly trusted and secure electronic identity means and trust services such as electronic signatures or attestations of attributes, expand citizens' possibilities to use them to access public and private online services and improve their ability to control when and with whom their personal identity data is accessed or shared.

Under the new Regulation, Member States would offer citizens and businesses digital identity wallets that would be able to link their national digital identity with proof of other personal attributes (e.g. driving licence, professional qualifications, bank credentials, attributes for medical use). These wallets may be provided by public authorities or by private entities, under the authority or recognised by a Member State. In line with the proposed Regulation, Member States will have to issue a wallet within 12 months of entry into force of the Regulation.

The European Digital Identity Wallets will enable EU citizens and residents to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they will have control of the data they share or grant access to. The European Digital Identity will be:

- **Available to anyone who wants to use it:** Any EU citizen, resident, and business in the Union who would like to make use of the European Digital Identity will be able to do so.
- **Widely useable:** The European Digital Identity wallets will be useable widely as a way either to identify users or to prove certain personal attributes, for the purpose of access to public and private digital services across the Union.
- **Designed in a way that assures users are in control of their data:** The European Digital Identity wallets will enable people to choose which aspects of their identity, data and certificates they share with third parties, and to keep track of such sharing. User control ensures that only information that needs to be shared will be shared.

The Toolbox Recommendation sets the framework for Member States to work together in close coordination with the Commission and other relevant stakeholders in order to develop a common Union toolbox to support the implementation of the European Digital Identity framework. The toolbox shall contain a comprehensive technical architecture and reference framework, a set of common standards and technical references and a set of guidelines and

³ [Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation \(EU\) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final](#)

⁴ [Commission Recommendation \(EU\) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework C\(2021\) 3968 final](#)

descriptions of best practices ('Common Union Toolbox'). Its scope should cover at least all aspects of the functionality of the European Digital Identity Wallets and of the qualified trust service for attestation of attributes as proposed by the Commission's proposal for a European Digital Identity framework. It is foreseen to publish the Common Union Toolbox in October 2022. The work on the Common Union Toolbox is carried out through the eIDAS Expert Group⁵.

The Digital Europe Work Programme 2021-2022 earmarks funding for procuring the development of the technical infrastructure to support interoperability and implementation of the European Digital Identity Wallet and its ecosystem as well as a reference application for the European Digital Identity Wallet to help Member States and other stakeholders implement the European Digital Identity framework. It is envisaged to make this reference application of the European Digital Identity Wallet available in Q4 2022 - Q1 2023.

3. **Security (law enforcement): AI-based pilots** - The digitalisation in all sectors and rapidly changing technological landscape bring along vast opportunities but unfortunately also create a fertile ground for criminals and terrorists. Law Enforcement Agencies (LEAs) often lack the necessary technical and financial means as well as digital skills when preventing, detecting, investigating or prosecuting criminal and terrorist activities supported by advanced technologies. In that context, supporting Member States' law enforcement (LE) cyber capacity building is paramount, in particular in the field of artificial intelligence (AI) applications that are key to address the data overload. The European Commission has put forward two complementary actions to support this policy. In the mid-term, the Data space for Security and the Law enforcement (see topic 2.2.1.12.2 of the Digital Europe Work Programme 2021-22) addresses the challenge of accessing relevant data sets to train and evaluate machine learning algorithms in the field of security. In the short term, as the subject of this topic, large scale pilots will enable the law enforcement to uptake AI solutions that already exist but are not yet validated in the police environment.

The Participation is open to all eligible entities as established by Article. 18 of the Digital Europe programme, in particular public sector as well as private sector organisations, including SMEs, NGOs and international organisations.

2. Objectives — Scope — Outcomes and deliverables — KPIs to measure outcomes and deliverables — Targeted stakeholders — Type of action — specific topic conditions

DIGITAL-2022-DEPLOY-02-EBSI-SERVICES – EBSI - Deployment of services

Objectives

The objective is to support through grants actions reinforcing EBSI and the EBP use cases. This will engage a large range of European actors in actions related to EBSI and EBP priorities⁶.

⁵ For information about the work of the Group, please consult [Register of Commission expert groups and other similar entities \(europa.eu\)](#).

⁶ See: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Learn+about+EBSI>

Scope

This topic will support the roll out of the EBSI by contributing to the implementation of at least one of following priorities:

1) EBSI nodes and support services

The aim is to support establishment, deployment and operation of EBSI nodes within EBP countries to enhance the performance, robustness, resilience, security and sustainability of EBSI and the provision of EBSI related services at national/local level in a coordinated way. The proposals shall seek to reinforce the coordination between EBSI nodes across Europe by sharing experiences, best practices and providing support services.

The supported nodes should become or contribute to the creation of EBSI competence centres in those countries, delivering support services to facilitate the exploitation of EBSI uptake at national and cross-border level, including different use cases and to contribute to the creation via EBSI of electronic ledgers as qualified trust services as foreseen in the proposal for the European Digital Identity Framework⁷. Such nodes would be considered as “reference nodes” for EBSI.

Support services can cover but are not limited to helpdesk services, training activities for local/national authorities, specific tools and technical resources that can assist public sector in adopting EBSI; as well as contributions to the EBSI network and the required cooperation and coordination including report and experience sharing for operating and enhancing the overall network.

All proposals addressing this priority are expected to be submitted by consortia regrouping EBSI nodes (established and/or to be established) from at least 7 EBP countries. All proposals are expected to work in a coordinated way with the EBSI core team and in particular the European Commission; and to be open to cooperating with other stakeholders or similar projects, to facilitate the integration of new nodes in the EBSI network and the exploitation of those nodes for users of EBSI.

Proposals submitted under this priority need to demonstrate that by the end of the Action the nodes are set up, operational, integrated with the EBSI and/or improved with enhanced technical features, in particular for security and sustainability aspects. They need to demonstrate as well their capacity to contribute to the overall enhancement of the EBSI and to its wide exploitation.

The indicative amount of funding expected to be allocated under this priority is approximately one third of the budget allocated to this topic.

2) Deployment of cross-border use cases

The aim is to support the deployment of specific cross-border use cases already selected by the European Blockchain Partnership (EBP)⁸.

The proposals shall seek to reinforce the coordination between actors involved in the deployment of the cross-border use cases by sharing experiences, best practices, users' engagement and providing support services to facilitate the exploitation of the

⁷ [COM\(2021\) 281 final: Proposal for a Regulation of the European Parliament and of the Council amending Regulation \(EU\) No 910/2014 as regards establishing a framework for a European Digital Identity](#)

⁸ At the time of launching of this call, the following seven use cases were selected by European Blockchain Partnership: Self-sovereign identity framework, Diploma (or the exchange of education and learning credentials), document traceability, European social security pass, SME financing, trusted data sharing which concerns in first steps asylum demand management and IOSS DR use case in the taxation area.

relevant use case leveraging EBSI capacities (i.e.g. information and training activities for potential users, etc.). They should ensure progress for business, functional or technical requirements, where appropriate providing solutions or components that can be integrated in the EBSI.

All proposals must include development, testing and deployment activities that exploit existing EBSI capabilities⁹. The proposals are encouraged to work on the development of the new EBSI capabilities and be ready to exploit them once available.

All proposals are expected to participate in coordinated actions, like the EBSI adopter programme¹⁰, that facilitate piloting and future exploitation of EBSI use cases. Those actions are driven by EBP representatives and/or within the EBSI core team, in cooperation with the European Commission. Consortium should be open to share the outcomes of their work and to cooperate with other stakeholders to facilitate the wide exploitation of EBSI use cases all across Europe.

Within this priority, 2 types of proposals are foreseen to be funded (depending on the use case covered):

i. Leveraging the work on verifiable credentials of the EBSI's Diploma and the European Social Security Pass use cases

Proposals leveraging the work of the EBSI's capacities and use cases concerning exchange of Verifiable Credentials already done in the context of the European Self Sovereign Identity Framework (eSSIF) and in the exchange of educational and life-learning credentials (Diploma use case) and the European Social Security Pass use cases will be supported under this topic in order to prepare for a large scale exploitation into production. This includes additional business requirements, scaling up of the activities, involvement of additional stakeholders, reinforcement the governance for the use case or communication activities.

All proposals addressing the above use cases are expected to be submitted by applicants from at least 7 EBP countries. All proposals are expected to work in a coordinated way with the EBSI core team and in particular the European Commission; and to be open to cooperating with other stakeholders or similar projects with a view of future extension of the use case to other EBP countries.

Applicants that intend to submit proposals related to the piloting of the first implementation of the European Digital Identity Wallet and its APIs should do it under the topic "DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID - Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation". All relevant projects concerning the two topics (EBSI and Electronic ID) are invited to propose appropriate coordination mechanism ensuring alignment between the work of the EBSI use case and the activities carried out in relation to European Digital Identity wallet, and to take into account relevant EU policies and initiatives.

The indicative amount of funding expected to be allocated under this priority is approximately one third of the budget allocated to this topic.

⁹ Existing EBSI capabilities are available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Learn+about+EBSI>

¹⁰ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Early+Adopters+Programme>

ii. Other use cases

Regarding the other EBP use cases for which more work still has to be done in the context of EBSI and its early adopter programme, such as document traceability¹¹, SME financing and trusted data sharing between authorities for asylum demand management, proposals should address the participation in the definition and implementation of the use cases, including business, functional and technical requirements, exploiting existing EBSI capabilities, and where appropriate, the provision of additional components that can be integrated into the EBSI. The objective is to launch pilot actions involving significant stakeholders with the view to enable the large scale implementation of the use case.

Use cases, other than the ones already selected by the EBP, could be supported if the usage of the EBSI is demonstrated and the EBP future endorsement is foreseen by the proposal.

All proposals addressing ii “other use cases” are expected to be submitted by applicants from at least 3 EBP countries. All proposals are expected to work in a coordinated way with the EBSI core team and in particular the European Commission; and to be open to cooperating with other stakeholders or similar projects with a view of future extension of the use case to other EBP countries.

The indicative amount of funding expected to be allocated under this priority is approximately one third of the budget allocated to this topic.

Outcomes and deliverables

EBSI is already developing use cases in cooperation with Member States and other Commission Services where significant resources have been invested and will need continued support until deployment for business continuity reasons. EBSI will support these cross border services and applications leveraging the EBP priorities.

It will reinforce the catalytic role of EBSI for providing better services to citizens and opportunities for businesses.

The projects should reinforce the EBSI and progress the deployment and the extension of the EBP use cases. They should deliver (depending on the priorities pursued):

- New EBSI nodes that enhance EBSI performance and robustness and establishing a network of reference nodes for EBSI in as many EBP countries as possible;
- Local EBSI support services that contribute to the EBSI enhancement and uptake at the national and cross-border level, facilitating as well the coordination with the EBSI team and the European Commission;
- Deployment of cross-border user cases, by contributing to the further development, piloting and operational exploitation of the EBP priority use cases.

Based on their EBSI experience, all projects should provide recommendations for the further development of the EBSI eco-system (see section 10).

¹¹ Document traceability refers to a large context: e.g. with documents concerning citizen or organisation activities like tracing across borders the authenticity of a mandate, or documents concerning the cross border traceability of products or objects.

KPIs to measure outcomes and deliverables

The projects should contribute to the reinforcement and wide exploitation of EBSI that will be appraised through the following KPIs:

- Number of EBSI nodes deployed and/or enhanced; including the number of reference nodes for EBSI
- Number of EBSI trainings focused done at national or sectoral level, complementing activities undertaken by the EBSI core team;
- Number of use cases piloted, and for each of them number of Member States that took part in the piloting of cross-border use cases, number of organisations involved and end users (i.e. end beneficiaries of the service)

Other KPIs for EBSI can be proposed by proposals to be used and/or developed during the lifetime of the projects.

Targeted stakeholders

In line with the specific type of proposals (as indicated under scope section), the consortium should include a mix of different stakeholders necessary for the deployment/operation of the EBSI nodes and/or the deployment of the cross-border use cases. Participating organisations should demonstrate complementary roles in the proposal, allowing for the comprehensive piloting of the EBSI capabilities with the ambition to contribute to and accelerate the exploitation EBSI and its use cases at a large scale. The applicants are encouraged to work together with the EBP representatives prior to the submission of the proposals. The following types of stakeholders are encouraged to apply (as part of the consortium):

- Member states authorities (at different level);
- Public and Private sector service providers;
- Node operators;
- Attribute/Attestations/Credentials Providers;
- Digital Wallet providers.

Other organisations are also encouraged to participate, in particular the organisations that are necessary for the piloting of specific use cases, including application services providers or issuers, end beneficiaries or verifiers, as well as solution providers. The direct involvement in projects of end users participating in pilot or exploitation of a use case is expected. It concerns both organisations or stakeholders having already experience with the deployment of EBSI at infrastructure or use case level, from other electronic ledger at infrastructure or use case level, or new ones and that aims to contribute to EBSI.

Type of action

Simple Grants — 50% funding rate

 For more information on Digital Europe types of action, see Annex 1.

Specific topic conditions

- For this topic, multi-beneficiary applications are mandatory and specific For this topic, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (see section 6)

- For this topic, following reimbursement option for equipment costs applies: depreciation only (*see section 10*)
- For this topic, access rights to ensure continuity and interoperability obligations apply (*see section 10*)
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
 - extent to which the project would reinforce and secure the digital technology supply chain in the Union*
 - extent to which the proposal can overcome financial obstacles such as the lack of market finance*

DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD – **Blockchain Standardisation**

Objectives

The objective of this topic is to three-fold: (i) to contribute towards implementing the Blockchain chapter of the Rolling Plan for ICT standardisation, (ii) to reinforce the link between EBSI and International and European blockchain/Distributed Ledger Technologies (DLT) standardisation and technical specification activities, (iii) strengthen participation of European start-ups, SMEs and independent experts in developing blockchain/DLT standards and technical specifications.

Scope

This action will involve and empower European stakeholders, participating in the development of open technical specifications and standards, to leverage on the work of EBSI (including best practices and use-cases) that takes into account European values and ethics, strengths the take-up, scalability, sustainability, security and interoperability of blockchain/DLT technological solutions.

The aim is to:

- support the implementation of the Rolling Plan for ICT Standardisation (in particular the Blockchain chapter) in International and European blockchain/DLT standardisation scenes;
- reinforce the link with EBSI and the European Blockchain Partnership (EBP);
- support the participation of European standardisation experts, in particular from European start-ups, SMEs and independent experts but as well from industry, research, education and governmental bodies, in International and European Standard Developing Organisations.

Key tasks to be carried out are:

- Mapping of the on-going activities in blockchain/DLT standardisation and technical specification;
- Setting up of a coordination facility liaising with relevant on-going developments in EU and national funded R&I projects, in particular with projects having identified standardisation output or with potential relevant

results, including as well other coordination and support actions, and relevant European Partnerships;

- Supporting participation and leadership (e.g. chairing of technical committees) of European experts in the organisations and activities (e.g. through working groups, technical bodies or committees) identified by the mapping. The aim should be to achieve critical mass from European independent experts, start-ups, SMEs, as well from industry, governmental bodies, research and academia for blockchain/DLT standardisation activities. This could include specific support to travel and accommodation costs¹² as well as specific work/service contracts¹³ to reinforce this participation;
- Reinforcing European values, ethics and policies e.g. for sustainability (green deal), technological sovereignty in blockchain/DLT standardisation.
- Promoting the benefits of blockchain/DLT standardisation and the contribution of EBSI, especially for SMEs, industry, research, education and governmental bodies; this will include actions, including development of tools and materials, to promote education on blockchain/DLT standardisation.

The proposals should take into account the activities carried out by:

- European Blockchain Services Infrastructure¹⁴;
- StandICT.eu 2023 project¹⁵ ;
- International Association for Trusted Blockchain Applications (INATBA)¹⁶;
- Blockchain Observatory and Forum¹⁷.

Outcomes and deliverables

Projects are expected to deliver to the following outcomes:

- Semi-annual mapping and expert activities reports of the relevant activities in blockchain/DLT standardisation with dedicated meetings to liaise with the European Commission, EBSI developers and blockchain standardisation experts;
- New contributions to the annual update of the Rolling Plan of ICT Standardisation and other relevant blockchain/DLT standardisation documents.

KPIs to measure outcomes and deliverables

- Number of supported experts participating in blockchain/DLT standardisation activities [Target: It is expected that 30 to 40 leading European experts would receive support via this call];
- Number of blockchain/DLT standardisation workshops/trainings/events organised [Target: It is expected that 2-4 main standardisation event/or workshops to be organised by the project];

¹² For meetings outside Europe, agreements need to be made in advanced with the Project Officer.

¹³ The consortium will define the process allowing to contribute to the funding of European experts to participate in blockchain/DLT standardisation activities to fulfil the scope of the call. The involvement and associated payment of the European experts needs to be done in line with the provisions of the grant agreement.

¹⁴ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>

¹⁵ <http://www.standict.eu>

¹⁶ <https://inatba.org/>

¹⁷ <https://www.eublockchainforum.eu>

- Number of contributions¹⁸ [Target: It is expected that 60 to 100 contributions will be done through Standardisation Deliverables/Technical reports contributed to per standardisation body, in particular international SDOs (ISO, ITU-T, IEC), European SDOs (CEN/CENELEC, ETSI) and other technical specification bodies such as IEEE, OASIS, IETF, W3C and other relevant (approx. 2-3 contributions per expert)].

Targeted stakeholders

The consortium should include a mix of different stakeholders necessary for contributing to blockchain/DLT standardisation activities. Participating organisations should demonstrate complementary roles in the proposal, allowing for the comprehensive implementation of key tasks. The following types of stakeholders are in particular encouraged to apply:

- Member states authorities (at different level);
- Public and Private associations/service providers working with blockchain/DLT standardisation;
- Organisations that have experience in blockchain/DLT standardisation activities
- Participants of European collaborative research and innovation programmes i.e. Horizon 2020 and Horizon Europe;

Other organisations are also encouraged to apply, in particular entities with Blockchain/DLT development experience.

Type of action

Coordination and Support Actions — 100% funding rate

 For more information on Digital Europe types of action, see Annex 1.

Specific topic conditions

- For this topic, following reimbursement option for equipment costs applies: depreciation only (see section 10)
- For this topic, access rights to ensure continuity and interoperability obligations apply (see section 10)
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
 - extent to which the project would reinforce and secure the digital technology supply chain in the Union*
 - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
 - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

¹⁸ The contribution is understood as acting as the project leader or at least preparing the text of significant part of standardisation deliverable/technical report. Just participating in the technical committee/working group meeting is not sufficient to be considered as a contribution for the purpose of this call.

DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID - Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation**Objectives**

The topic aims to support the piloting of the European Digital Identity Wallets (the Wallets) by Member States and relevant stakeholders in compliance with the common Union toolbox and the reference application of the Wallet which will be made available to Member States.

For this purpose, it will promote the development and deployment of use-cases for the new European Digital Identity ecosystem in different areas involving both public and private sector stakeholders. It aims to test the interoperability and scalability of the developed solutions within their national and cross-border implementation contexts, trial user journeys, collect feedback as appropriate for iterative updates of the toolbox and the reference application of the Wallet, and promote the opportunities of the new infrastructure among public and private sector stakeholders and users. Overall the topic should help Member States build the necessary expertise and infrastructure to facilitate the provision of Wallets following the relevant obligations which are to be set-out in the future Regulation.

Scope

Building on the proposal for a European Digital Identity Framework and the Recommendation for a Union Toolbox for a coordinated approach towards a European Digital Identity Framework, the topic will support usage scenarios of the Wallet in order to validate and facilitate the implementation of the reference application of the Wallet, to be developed based on the common Union Toolbox. Specifically, beneficiaries will coordinate implementation activities by public and private sector service providers to integrate their systems with the Wallet and its ecosystem for the purpose of the exchange of digital attestations of attributes and credentials as defined in the new Regulation¹⁹.

Proposals should cover in particular the mobile driving licence, payments, eHealth, and educational and qualifications (diploma) usage scenarios. Proposals may also address other use cases.

To ensure common implementation of the European Digital Identity framework, all projects must integrate with the iterative development of the reference application of the Wallet, to be developed on the basis of the Architecture and Reference Framework (ARF) foreseen to be published under the Toolbox Recommendation in October 2022. Proposals should be aligned with the outline of the ARF²⁰ and describe the process of integration with the development of the reference application of the Wallet.

Where appropriate, proposals should build on pre-existing work and make use of existing infrastructures. Applicants should also ensure alignment with other ongoing cross-border initiatives and take advantage of synergies that could emerge with activities financed through other grants in the same domain and indicate stakeholders that will be consulted during the execution of the proposed project.

¹⁹ As defined in [Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation \(EU\) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final](#)

²⁰ <https://futurium.ec.europa.eu/en/digital-identity>

Moreover, the proposals shall include:

- The implementation of onboarding procedures for Wallet Users, providers of electronic attestations of attributes (EAA), qualified electronic attestations of attributes (QEAA) and credentials, and relying parties;
- The integration of the interfaces of relying parties and EAA, QEAA and credential issuers to the Wallet in their pre-production systems;
- The trialling of user journeys involving relevant core functionalities of the Wallet;
- Comprehensive testing of the cross-border functionality of Wallets in a pre-production environment demonstrating readiness to progress into production;
- Cooperation with the Commission to integrate with the iterative development of the reference application of the Wallet including the successful integration of new releases of APIs for:
 - requesting EAAs, QEAs and credentials, presentation and validation of services (including connectivity and compliance tests)
 - issuing EAAs, QEAs and credentials (including connectivity and compliance tests).
- Completion of a sufficiently high number of cross-border transactions (i.e. with Issuers and Holders of EAAs, QEAs and credentials, Wallet Issuers and Relying Parties coming from at least 3 different eligible countries) to demonstrate the Wallet's functionalities.
- A roadmap for the implementation of, and recommendations for, the further development of the eco system and a sustainability strategy (as detailed under section 10).

Projects should ensure that the main roles in the Wallet ecosystem and the respective usage scenarios are filled by legally entitled organisations. Projects should be run in a pre-production environment, involving a sufficient number of Wallet Users in testing.

Outcomes and deliverables

Large-scale pilots demonstrating the functionality of the Wallet in national and cross-border contexts.

Pilots may focus on one or more of the following usage scenarios:

- **Mobile Driving Licence** - The wallet user can prove privileges to drive a vehicle to public or private sector entities;
- **Payments** - The wallet user can authorise payments for products or services online and at physical points of sale;
- **eHealth** - The wallet user can provide relevant attributes and/or authorisation to a healthcare provider to access a patient summary, a prescription for medicinal products, or other health data;

- **Education / Professional Qualification** - The wallet user can prove an educational or professional qualification to public or private sector entities ;
- **Other usage scenarios** – e.g. in the areas of digital travel credentials and social security. Such scenarios may also demonstrate the functionalities of the Wallet for example qualified electronic signatures.

KPIs to measure outcomes and deliverables

Proposals shall set targets for, measure and report on at least the following KPIs:

- Number of Wallet issuing countries involved in the project;
- Number of Wallet users of involved in the project;
- Number of relying parties having integrated interfaces to the Wallet in their pre-production systems;
- Number of Issuers of EAAs, QEAs and Credentials having integrated interfaces to the Wallet in their pre-production systems;
- Number of Wallet transactions completed in a pre-production environment;
- Where relevant for the proposal, number of qualified electronic signatures issued by users of the Wallet.

Targeted stakeholders

The topic targets proposals submitted by Governmental bodies responsible for issuing European Digital Identity Wallets.²¹

In addition, consortia should include the necessary natural and legal persons to ensure the required outcome. This may include:

- National agencies responsible for the implementation of relevant infrastructures and cross-border initiatives in the relevant domain
- Public and private relying parties, including but not restricted to those that are necessary for piloting a specific usage scenario²²
- Attribute/Credential/Attestation Providers
- Wallet Users – EU Citizens and Residents testing the functionalities of the Wallet

To allow for comprehensive cross-border piloting of the Wallets, proposals should include at least 3 countries performing the three roles defined below:

- **Wallet Issuing Country** – Country which is issuing a wallet throughout the project in alignment with the reference application of the Wallet;
- **Credential Issuing Country** – Country where an entity/entities issuing EAAs, QEAs and credentials is/are based;
- **Relying Party Country** – Country where a relying party/relying parties receiving credentials is/are based.

²¹ As defined in [Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation \(EU\) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final](#)

²² As defined in [COM\(2021\)281 final](#)

Applicants can increase the relevance of their proposals by including a higher number of countries performing all three of the above roles.

Type of action

Simple Grants — 50% funding rate

 For more information on Digital Europe types of action, see Annex 1.

Specific topic conditions

- For this topic, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (*see section 6*)
- For this topic, following reimbursement option for equipment costs applies: depreciation only (*see section 10*)
- For this topic, access rights to ensure continuity and interoperability obligations apply (*see section 10*)
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
 - extent to which the project would reinforce and secure the digital technology supply chain in the Union*
 - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
 - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI - Security (law enforcement): AI-based pilots

Objectives

The overall objective is to enable the final validation and to foster the uptake of artificial intelligence (AI) systems for law enforcement (LE) by running large scale pilots in Law Enforcement Agencies (LEAs)²³ premises. This is necessary, as AI systems for LE need, in most cases, a final validation on real operational datasets²⁴ that can only be accessed in stand-alone secured environments.

This action will contribute to close the gap between prototypes that have been developed with the support of EU funded security research and innovation programmes (i.e. up to TRL 7) and systems proven in operational environment that bring clear added value to police practitioners (i.e. TRL 8/9).

²³ In the context of this Topic, 'Law Enforcement Agencies' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences.

²⁴ In compliance with Directive 2016/680 of the European Parliament and the Council of 27 April 2016

Due to the sensitivity of data handled in investigations, this can only be done by LE, in their own premises and on real use cases. This is particularly true in the context of AI where the relevance of data sets plays an important role in avoiding inaccurate, biased or even discriminatory outcomes. Projects under this action should pay specific attention to fundamental rights challenges; for example, by proposing bias mitigation²⁵ and non-discrimination mechanisms²⁶ as well as by providing measures on data quality and protection. They should also provide elements on how the compliance with the EU legal framework on data processing for police purposes as set out in Directive 2016/680 of the European Parliament and the Council of 27 April 2016 and in the General Data Protection Regulation (GDPR) will be ensured.

From a data perspective, this action complements the creation of a Data space for Security and law enforcement. The Data space for Security and law enforcement will gather pseudo operational data (or anonymized datasets) that will be used to train and test AI systems, while this action will make full use of real operational data in stand-alone environments to assess, validate and better train AI systems.

Scope

To achieve the above mentioned objective, the funding will be granted to pilots which test, validate and optimise innovative digital forensic and investigation tools over sufficient periods of time (minimum 6 months) in real operational environment. Specific attention will be given to solutions that can benefit EU law enforcement at large, with a significant impact on the efficiency of digital investigations. Proposals should also give sufficient emphasis on how fundamental rights challenges will be addressed, for example by enhancing data quality, mitigating bias, detecting errors and avoiding any form of discrimination in the decision-making process.

Within the scope of this Topic, there are two categories of activities:

A. Proposals submitted under this topic **must** address the following activities:

1. Identifying and building on technologies that address the core functions of digital investigations (e.g. filtering and clustering illegal content, extracting name entities, finding patterns and correlations in unstructured datasets, etc....), with a preference for open source solutions, e.g. stemming from Horizon 2020 or Internal Security Fund Police programmes that can be available for the law enforcement at little or no cost;
2. Rolling out the selected solution (or set of tools) in law enforcement premises over at least a 6-month period;
3. Training (when relevant), adapting (when relevant) and evaluating the solutions on operational datasets and real use cases;
4. Demonstrating the compliance of the proposed solution in terms of usability, efficiency and compliance with EU standards as regards privacy and data protection and providing further feedback on parts of the solution to be improved if applicable;

²⁵ https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf

²⁶ https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf

5. Ensuring a permanent uptake of the solution after the piloting phase if the proposed solution fulfilled the requirements of usability, efficiency and compliance with EU standards as regards privacy and data protection;
6. Demonstrating that the proposed solution could benefit a number of EU LEAs, e.g. by prompting technical interoperability through standards or with the enforcement of intellectual property rights that favours the availability of solutions for EU LEAs at little or no cost.

B. Where relevant, proposals are also encouraged to:

1. Create a set of annotated data that could eventually be shared among LE and potentially Europol (and possibly feed the data space for security);
2. Develop and provide relevant trainings to law enforcement practitioners that could eventually be shared among LEAs and potentially CEPOL (European Union Agency for Law Enforcement Training) and ECTEG (European Cybercrime Training and Education Group);
3. Refer to the work carried out by the Europol Innovation Lab to identify innovative solutions that could fill LE capacity gaps, and possibly to use Europol Innovation Lab core groups as a structure for Member States to coordinate the creation of large-scale pilots AI systems for LE amongst themselves and to further disseminate the results of the pilots;
4. Refer to the work carried out by EACTDA (the European Anti-Cybercrime Technology Development Association);
5. Coordinate and create synergies with related activities in the Horizon 2020, Horizon Europe and Internal Security Fund Police programmes²⁷.

Outcomes and deliverables

The action will have direct impact on the capability of LE to deploy innovative solutions and thus to handle the abundance of digital evidence efficiently and in accordance with EU core values. In addition, it will contribute to foster the adoption and give visibility to best-in-class solutions developed in the EU.

The expected deliverables of the pilots **must** include the following in line with **activities (A)**:

1. The solution (or set of tools) rolled out and exploited for testing purposes in law enforcement premises over a 6-month period;
2. The context of use of the selected solution, its expected added value explained and measures taken to foster uptake at EU level;
3. Results of the evaluation and testing of the solution (or set of tools) including explanation of testing environment and applied methodology;
4. Software developments (if any) to enhance or adapt the solution to the context use (i.e. documentation and source code developed in the course of the pilots).

²⁷ Notably projects such as CYCLOPES, AIDA, GRACE, INFINITY and STARLIGHT.

Applicants are also encouraged to include the following deliverables in line with **activities (B)**:

1. Annotated data sets created in the course of the pilots with a report explaining the accuracy and compliance with EU core values, instructions for use, reference to standards and sharing rules (when relevant);
2. A report on trainings developed and conducted on the use of the solution (or set of tools) and feedback received from participants (including new training materials, if relevant);
3. A report on dissemination activities performed, synergies created with relevant institutions, networks of practitioners or EU funded projects and feedback received.

Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results, which should be reflected in the classification of deliverables and in the processes to handle project's materials.

KPIs to measure outcomes and deliverables

The expected KPIs corresponding to **activities (A)** must include:

1. Number of instance of tool(s) rolled out in law enforcement premises (a tool may be rolled out in several LE services): at least 1,
2. Number of users having a regular access to the tool(s) for testing purposes: at least 5 per tool,
3. Number of reports providing information on the testing environment, testing methodology and test results: at least 1.

Additional KPIs corresponding to **activities (B)** may include:

4. Number of annotated datasets created and shared among EU LEAs: at least 1,
5. Number of users trained to use the tool: at least 10 per tool,
6. Number of training materials elaborated: at least 1,
7. Number of innovative tools that are kept after the end of the pilots by LEAs for permanent use: at least 1,
8. Number of innovative tools that are made available to EU law enforcement, e.g. through Europol repository for tools or through the EACTDA (European Anti-Cybercrime Technology Development Association): at least 1,
9. Number of dissemination activities conducted (e.g. number of meetings with other LE agencies, network of practitioners or other relevant entities): at least 4.

Targeted stakeholders

This action targets pre-eminently law enforcement agencies that will be the main beneficiary of the projects' outcomes.

Law enforcement shall be supported by public or private entities from eligible countries participating in the programme notably on technical aspects (e.g. to install, configure, possibly develop solutions or create datasets), legal aspects (e.g. to ensure

compliance with EU regulations or prepare impact assessment in relation with data protection obligations) or to provide trainings.

Relevant associations in the field, such as EACTDA (European Anti-Cybercrime Technology Development Association), ECTEG (European Cybercrime Training and Education Group) or ENFSI (European Network of Forensic Science Institutes) could also play a role in the projects, for example, to coordinate with existing activities of a similar nature or to foster the dissemination of project outcomes.

The participation of Small and Medium Enterprises (SMEs) is highly encouraged.

Type of action

SME Support Actions — 50% and 75% (for SMEs) funding rate

 For more information on Digital Europe types of action, see Annex 1.

Specific topic conditions

- For this topic, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (see section 6)
- For this topic, the following reimbursement option for equipment costs applies: full costs only (see section 10)
- For this topic, access rights to ensure continuity and interoperability obligations apply (see section 10)
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
 - extent to which the project would reinforce and secure the digital technology supply chain in the Union*
 - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
 - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

3. Available budget

The available call budget is **EUR 58 000 000**. This budget might be increased by maximum 20%.

Specific budget information per topic can be found in the table below.

Topic	Topic budget
1. DIGITAL-2022-DEPLOY-02-EBSI-SERVICES	EUR 15 000 000
2. DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD	EUR 1 000 000
3. DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID	EUR 37 000 000

4. DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI	EUR 5 000 000
---	----------------------

We reserve the right not to award all available funds or to redistribute them between the call priorities, depending on the proposals received and the results of the evaluation.

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	22 February 2022
<u>Deadline for submission:</u>	<u>17 May 2022 – 17:00:00 CEST (Brussels local time)</u>
Evaluation:	June – July 2022
Information on evaluation results:	August 2022
GA signature:	December 2022

5. Admissibility and documents

Proposals must be submitted before the **call deadline** (see *timetable section 4*).

Proposals must be submitted **electronically** via the Funding & Tenders Portal Electronic Submission System (accessible via the Topic page in the [Search Funding & Tenders](#) section). Paper submissions are NOT possible.

Proposals (including annexes and supporting documents) must be submitted using the forms provided *inside* the Submission System (⚠ NOT the documents available on the Topic page — they are only for information).

Proposals must be **complete** and contain all the requested information and all required annexes and supporting documents:


- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project (*to be filled in directly online*)
- Application Form Part B — contains the technical description of the project (*to be downloaded from the Portal Submission System, completed and then assembled and re-uploaded*)
- **mandatory annexes and supporting documents** (*to be uploaded*):
 - detailed budget table: not applicable
 - CVs of core project team: not applicable
 - activity reports of last year: not applicable
 - list of previous projects: not applicable
 - **security issues table: applicable**
 - **ethics issues table: applicable**
 - ownership control declaration: not applicable

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover you will have to confirm that the information in the application is correct and complete and that the participants comply with the conditions for receiving EU funding (especially eligibility, financial and operational capacity, exclusion, etc). Before signing the grant, each beneficiary and affiliated entity will have to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable, accessible and printable**.

Proposals for Simple Grants and SME Support Actions are limited to maximum **70 pages** (Part B). Proposals for Coordination and Support Actions are limited to maximum **50 pages** (Part B). Evaluators will not consider any additional pages.

You may be asked at a later stage for further documents (*for legal entity validation, financial capacity check, bank account validation, etc*).

 For more information about the submission process (including IT aspects), consult the [Online Manual](#).

6. Eligibility

Eligible participants (eligible countries)

In order to be eligible, the applicants (beneficiaries and affiliated entities) must:

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e.:
 - EU Member States (including overseas countries and territories (OCTs))
 - non-EU countries:
 - listed EEA countries and countries associated to the Digital Europe Programme or countries which are in ongoing negotiations for an association agreement and where the agreement enters into force before grant signature ([list of participating countries](#)^(OBJ))

Beneficiaries and affiliated entities must register in the [Participant Register](#) — before submitting the proposal — and will have to be validated by the Central Validation Service (REA Validation). For the validation, they will be requested to upload documents showing legal status and origin.

Other entities may participate in other consortium roles, such as associated partners, subcontractors, third parties giving in-kind contributions, etc (*see section 13*).

Specific cases

Natural persons — Natural persons are NOT eligible (with the exception of self-employed persons, i.e. sole traders, where the company does not have legal personality separate from that of the natural person).

International organisations — International organisations are not eligible, unless they are International organisations of European Interest within the meaning of Article 2 of the Digital Europe Regulation (i.e. international organisations the majority of whose members are Member States or whose headquarters are in a Member State).

Entities without legal personality — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees

for the protection of the EU financial interests equivalent to that offered by legal persons²⁸.

EU bodies — EU bodies (with the exception of the European Commission Joint Research Centre) can NOT be part of the consortium.

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'²⁹. ⚠ Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

Countries currently negotiating association agreements — Beneficiaries from countries with ongoing negotiations (*see above*) may participate in the call and can sign grants if the negotiations are concluded before grant signature (with retroactive effect, if provided in the agreement).

EU restrictive measures — Special rules apply for certain entities (*e.g. entities subject to [EU restrictive measures](#) under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)*³⁰ and entities covered by Commission Guidelines No [2013/C 205/05](#)³¹). Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

 For more information, see [Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment](#).

Consortium composition

Proposals must be submitted by:

for topic **DIGITAL-2022-DEPLOY-02-EBSI-SERVICES:**

- Minimum 3 applicants (beneficiaries; not affiliated entities) from 3 different eligible countries.

for topic **DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID:**

- Minimum 3 applicants from 3 different eligible countries.

for topic **DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI:**

- Minimum 2 law enforcement agencies (beneficiaries; not affiliated entities).

Eligible activities

Eligible activities are the ones set out in section 2 above.

Projects should take into account the results of projects supported by other EU funding programmes. The complementarities must be described in the project proposals (Part B of the Application Form).

²⁸ See Article 197(2)(c) EU Financial Regulation [2018/1046](#).

²⁹ For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation [2018/1046](#).

³⁰ Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the [EU Sanctions Map](#).

³¹ Commission guidelines No [2013/C 205/05](#) on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards (OJEU C 205 of 19.07.2013, pp. 9-11).

Projects must comply with EU policy interests and priorities (*such as environment, social, security, industrial and trade policy, etc*).

Ethics

Projects must comply with:

- highest ethical standards and
- applicable EU, international and national law (including the [General Data Protection Regulation 2016/679](#)).

Proposals under this call for proposals will have to undergo an ethics review to authorise funding and may be made subject to specific ethics rules (which become part of the Grant Agreement in the form of ethics deliverables, *e.g. ethics committee opinions/notifications/authorisations required under national or EU law*).

For proposals involving development, testing, deployment, use or distribution of AI systems, the ethics review will in particular check compliance with the principles of human agency and oversight, diversity/fairness, transparency and responsible social impact, while the experts performing the technical evaluation will assess the robustness of the AI systems (i.e. their reliability not to cause unintentional harm).

Security

Projects involving EU classified information must undergo security scrutiny to authorise funding and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

These rules (governed by Decision [2015/444](#)³² and its implementing rules and/or national rules) provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded
- classified information must be marked in accordance with the applicable security instructions in the SAL
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:
 - created or accessed only on premises with facility security clearing (FSC) from the competent national security authority (NSA), in accordance with the national rules
 - handled only in a secured area accredited by the competent NSA
 - accessed and handled only by persons with valid personnel security clearance (PSC) and a need-to-know
- at the end of the grant, the classified information must either be returned or continue to be protected in accordance with the applicable rules
- action tasks involving EU classified information (EUCI) may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative

³² See Commission Decision 2015/544/EU, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

arrangement with the Commission)

- disclosure of EUCI to third parties is subject to prior written approval from the granting authority.

Please note that, depending on the type of activity, facility security clearing may have to be provided before grant signature. The granting authority will assess the need for clearing in each case and will establish their delivery date during grant preparation. Please note that in no circumstances can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearing.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables (*e.g. create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc*).

Beneficiaries must ensure that their projects are not subject to national/third-country security requirements that could affect implementation or put into question the award of the grant (*e.g. technology restrictions, national security classification, etc*). The granting authority must be notified immediately of any potential security issues.

7. Financial and operational capacity and exclusion

Financial capacity

Applicants must have **stable and sufficient resources** to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all these projects.

The financial capacity check will be carried out on the basis of the documents you will be requested to upload in the [Participant Register](#) during grant preparation (*e.g. profit and loss account and balance sheet, business plan, audit report produced by an approved external auditor, certifying the accounts for the last closed financial year, etc*). The analysis will be based on neutral financial indicators, but will also take into account other aspects, such as dependency on EU funding and deficit and revenue in previous years.

The check will normally be done for all beneficiaries, except:

- public bodies (entities established as public body under national law, including local, regional or national authorities) or international organisations
- if the individual requested grant amount is not more than EUR 60 000.

If needed, it may also be done for affiliated entities.

If we consider that your financial capacity is not satisfactory, we may require:

- further information
- an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities (*see below, section 10*)
- prefinancing paid in instalments
- (one or more) prefinancing guarantees (*see below, section 10*)

or

- propose no prefinancing
- request that you are replaced or, if needed, reject the entire proposal.

 For more information, see [Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment](#).

Operational capacity

Applicants must have the **know-how, qualifications** and **resources** to successfully implement the projects and contribute their share (including sufficient experience in projects of comparable size and nature).

This capacity will be assessed together with the 'Implementation' award criterion, on the basis of the competence and experience of the applicants and their project teams, including operational resources (human, technical and other) or, exceptionally, the measures proposed to obtain it by the time the task implementation starts.

If the evaluation of the award criterion is positive, the applicants are considered to have sufficient operational capacity.

Applicants will have to show their capacity via the following information:

- general profiles (qualifications and experiences) of the staff responsible for managing and implementing the project
- description of the consortium participants

Additional supporting documents may be requested, if needed to confirm the operational capacity of any applicant.

Exclusion

Applicants which are subject to an **EU exclusion decision** or in one of the following **exclusion situations** that bar them from receiving EU funding can NOT participate³³:

- bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)
- in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)
- guilty of grave professional misconduct³⁴ (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

³³ See Articles 136 and 141 of EU Financial Regulation [2018/1046](#).

³⁴ Professional misconduct includes: violation of ethical standards of the profession, wrongful conduct with impact on professional credibility, false declarations/misrepresentation of information, participation in a cartel or other agreement distorting competition, violation of IPR, attempting to influence decision-making processes or obtain confidential information from public authorities to gain advantage.

- guilty of irregularities within the meaning of Article 1(2) of Regulation No [2988/95](#) (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant).

Applicants will also be refused if it turns out that³⁵:

- during the award procedure they misrepresented information required as a condition for participating or failed to supply that information
- they were previously involved in the preparation of the call and this entails a distortion of competition that cannot be remedied otherwise (conflict of interest).

8. Evaluation and award procedure

The proposals will have to follow the **standard submission and evaluation procedure** (one-stage submission + one-step evaluation).

An **evaluation committee** (assisted by independent outside experts) will assess all applications. Proposals will first be checked for formal requirements (admissibility, and eligibility, see *sections 5 and 6*). Proposals found admissible and eligible will be evaluated (for each topic) against the operational capacity and award criteria (see *sections 7 and 9*) and then ranked according to their scores.


For proposals with the same score (within a topic or budget envelope) a **priority order** will be determined according to the following approach:

Successively for every group of *ex aequo* proposals, starting with the highest scored group, and continuing in descending order:

- 1) Proposals focusing on a theme that is not otherwise covered by higher ranked proposals will be considered to have the highest priority.
- 2) The *ex aequo* proposals within the same topic will be prioritised according to the scores they have been awarded for the award criterion 'Relevance'. When these scores are equal, priority will be based on their scores for the criterion 'Impact'. When these scores are equal, priority will be based on their scores for the criterion 'Implementation'.
- 3) If this does not allow to determine the priority, a further prioritisation can be done by considering the overall proposal portfolio and the creation of positive synergies between proposals, or other factors related to the objectives of the call. These factors will be documented in the panel report.
- 4) After that, the remainder of the available call budget will be used to fund projects across the different topics in order to ensure a balanced spread of the geographical and thematic coverage and while respecting to the maximum possible extent the order of merit based on the evaluation of the award criteria.

³⁵ See Article 141 EU Financial Regulation [2018/1046](#).

All proposals will be informed about the evaluation result (**evaluation result letter**). Successful proposals will be invited for grant preparation; the other ones will be put on the reserve list or rejected.

 No commitment for funding — Invitation to grant preparation does NOT constitute a formal commitment for funding. We will still need to make various legal checks before grant award: *legal entity validation, financial capacity, exclusion check, etc.*

Grant preparation will involve a dialogue in order to fine-tune technical or financial aspects of the project and may require extra information from your side. It may also include adjustments to the proposal to address recommendations of the evaluation committee or other concerns. Compliance will be a pre-condition for signing the grant.

If you believe that the evaluation procedure was flawed, you can submit a **complaint** (following the deadlines and procedures set out in the evaluation result letter). Please note that notifications which have not been opened within 10 days after sending are considered to have been accessed and that deadlines will be counted from opening/access (see also [Funding & Tenders Portal Terms and Conditions](#)). Please also be aware that for complaints submitted electronically, there may be character limitations.

9. Award criteria

The **award criteria** for this call are as follows:

- **Relevance**
 - Alignment with the objectives and activities as described in section 2
 - Contribution to long-term policy objectives, relevant policies and strategies, and synergies with activities at European and national level
 - Extent to which the project would reinforce and secure the digital technology supply chain in the EU*
 - Extent to which the project can overcome financial obstacles such as the lack of market finance*
- **Implementation**
 - Maturity of the project
 - Soundness of the implementation plan and efficient use of resources
 - Capacity of the applicants, and when applicable the consortium as a whole, to carry out the proposed work
- **Impact**
 - Extent to which the project will achieve the expected outcomes and deliverables referred to in the call for proposals and, where relevant, the plans to disseminate and communicate project achievements
 - Extent to which the project will strengthen competitiveness and bring important benefits for society

- Extent to which the project addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects *.

**May not be applicable to all topics (see specific topic conditions in section 2).*

Award criteria	Minimum pass score	Maximum score
Relevance	3	5
Implementation	3	5
Impact	3	5
Overall (pass) scores	10	15

Maximum points: 15 points.

Individual thresholds per criterion: 3/5, 3/5 and 3/5 points.

Overall threshold: 10 points.

Proposals that pass the individual thresholds AND the overall threshold will be considered for funding — within the limits of the available call budget. Other proposals will be rejected.

10. Legal and financial set-up of the Grant Agreements

If you pass evaluation, your project will be invited for grant preparation, where you will be asked to prepare the Grant Agreement together with the EU Project Officer.

This Grant Agreement will set the framework for your grant and its terms and conditions, in particular concerning deliverables, reporting and payments.

The Model Grant Agreement that will be used (and all other relevant templates and guidance documents) can be found on [Portal Reference Documents](#).

Starting date and project duration

The project starting date and duration will be fixed in the Grant Agreement (*Data Sheet, point 1*). Normally the starting date will be after grant signature. Retroactive application can be granted exceptionally for duly justified reasons but never earlier than the proposal submission date.

Indicative Project duration:

- **DIGITAL-2022-DEPLOY-02-EBSI-SERVICES** between 18 and 24 months.
- **DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD** 24 months.
- **DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID** 24 months.
- **DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI** 24 months.

Extensions are possible, if duly justified and through an amendment.

Milestones and deliverables

The milestones and deliverables for each project will be managed through the Portal Grant Management System and will be reflected in Annex 1 of the Grant Agreement.

The following deliverable will be mandatory for all projects:

- additional deliverable on dissemination and exploitation, to be submitted in the first six months of the project

The following deliverables will be mandatory for **DIGITAL-2022-DEPLOY-02-EBSI-SERVICES**

- The interim and final reports should address (the list of points is not exhaustive) :
 - The engagement with stakeholders and their relevance for the EBSI take-up;
 - Legal, technical and organisational challenges, including security and data protection considerations and future standardisation needs. Appropriate follow up should be identified;
 - Recommendations for the further development of the EBSI eco-system;
 - Specific organisational structure and governance procedures;
 - Deliverables and achievements;
 - Synergies with other actions;
 - Updated KPIs;
 - Information on how dissemination and exploitation plans were implemented.

The following deliverables will be mandatory for **DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD**

- Periodic reports (semi-annual) providing an overview and numbers concerning:
 - Mapping activities in blockchain/DLT standardisation, including those relevant to the Rolling Plan of ICT Standardisation and to EBSI;
 - Supported Experts participating in blockchain/DLT standardisation activities;
 - Standardisation Committees/Working groups contributed to;
 - Leadership positions in Standardisation Committees/Working groups;
 - Standardisation Deliverables/Technical reports contributed to per standardisation body/technical committee/working group, in particular International SDOs (ISO, ITU-T, IEC), European SDOs (CEN/CENELEC, ETSI) and other technical specification bodies such as IEEE, OASIS, IETF, W3C and other relevant;
 - Synergies with other relevant initiatives or European players including from EU (and national) funded R&I projects;
 - Blockchain/DLT standardisation workshops/trainings/events organised, as well as the number of participants per workshop/training/event;

- Liaison sessions/trainings with EBSI experts involving the European Commission;
- Contributions to drafting the Blockchain chapter of the Rolling Plan of ICT Standardisation and other relevant blockchain/DLT standardisation documents;
- Actions of the Blockchain chapter of the Rolling Plan of ICT Standardisation on which project has made a substantial implementation effort;
- Supported Blockchain/DLT standardisation meetings (listening experts supported);
- Awareness and education activities on blockchain/DLT standardisation.

The following deliverables will be mandatory for **DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID**

- A roadmap for the implementation of the eco-system. The roadmap should include at least:
 - An analysis of stakeholders and their relevance for the take-up of the Digital Identity Wallet;
 - Legal, technical and organisational challenges, including security and data protection considerations and future standardisation needs. Appropriate follow up should be identified;
 - The planned organisational structure and governance procedures;
 - Outline of the future implementation support;
 - Accompanying evaluation and monitoring activities.
- Sustainability business strategy setting out potential business and revenue models, including estimates on the number users expected to be able to download/share personal identification data, the EAAs, QEAAAs and Credentials relevant to the usage scenarios into their Wallets;
- Periodic reports (semi-annual) providing an overview and numbers:
 - Participating beneficiaries in a usage scenario implementation;
 - Role of beneficiaries participating in a usage scenario implementation;
 - Leading beneficiaries in usage scenarios implementation;
 - Usages Scenario workshops/trainings/events organised, as well as the number of participants per workshop/training/event;
 - Liaison sessions/trainings with eIDAS experts involving the European Commission;
 - Outcomes and Deliverable as set out in Section 2;
 - KPIs to measure outcomes and deliverables as set out in Section 2;
- Final report at the completion of a project detailing the project's results and providing recommendations on the further development of the European Digital Identity Framework ecosystem.

Form of grant, funding rate and maximum grant amount

The grant parameters (*maximum grant amount, funding rate, total eligible costs, etc.*) will be fixed in the Grant Agreement (*Data Sheet, point 3 and art 5*).

Indicative Project budget (maximum grant amount):

- **DIGITAL-2022-DEPLOY-02-EBSI-SERVICES** applicants can request up to EUR 5 000 000 per project.
- **DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD** EUR 1 000 000 per project.
- **DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID** between EUR 10 00 000 and EUR 12 000 000 per project.
- **DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI** applicants can request up to EUR 5 000 000 per project.

The grant awarded may be lower than the amount requested.

The grant will be a budget-based mixed actual cost grant (actual costs, with unit cost and flat-rate elements). This means that it will reimburse ONLY certain types of costs (eligible costs) and costs that were *actually* incurred for your project (NOT the *budgeted* costs). For unit costs and flat-rates, you can charge the amounts calculated as explained in the Grant Agreement (*see art 6 and Annex 2 and 2a*).

The costs will be reimbursed at the funding rate fixed in the Grant Agreement. This rate depends on the type of action which applies to the topic, *see section 2*. Grants may NOT produce a profit (i.e. surplus of revenues + EU grant over costs). For-profit organisations must declare their revenues and, if there is a profit, we will deduct it from the final grant amount (*see art 22.3*).

Moreover, please be aware that the final grant amount may be reduced in case of non-compliance with the Grant Agreement (*e.g. improper implementation, breach of obligations, etc.*).

Budget categories and cost eligibility rules

The budget categories and cost eligibility rules are fixed in the Grant Agreement (*Data Sheet, point 3 and art 6*).

Budget categories for this call:

- A. Personnel costs
 - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
 - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
 - C.1 Travel and subsistence
 - C.2 Equipment
 - C.3 Other goods, works and services
- D. Other cost categories
 - D.1 Financial support to third parties: not applicable

- D.2 Internally invoiced goods and services
- E. Indirect costs

Specific cost eligibility conditions for this call:

- personnel costs:
 - average personnel costs (unit cost according to usual cost accounting practices): Yes
 - SME owner/natural person unit cost³⁶: Yes
- travel and subsistence unit costs³⁷: No (only actual costs)
- equipment costs:
 - depreciation for topics: **DIGITAL-2022-DEPLOY-02-EBSI-SERVICES, DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD, and DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID**
 - full cost for topic: **DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI**
- other cost categories:
 - costs for financial support to third parties: not allowed.
 - internally invoiced goods and services (costs unit cost according to usual cost accounting practices): Yes
- indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any).
- VAT: non-deductible VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
- other:
 - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
 - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed
 - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for *separate* project websites are not eligible

Reporting and payment arrangements

The reporting and payment arrangements are fixed in the Grant Agreement (*Data Sheet, point 4 and art 21 and 22*).

After grant signature, you will normally receive a **prefinancing** to start working on the project (float of normally **50%** of the maximum grant amount; exceptionally less

³⁶ Commission [Decision](#) of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7715).

³⁷ Commission [Decision](#) of 12 January 2021 authorising the use of unit costs for travel, accommodation and subsistence costs under an action or work programme under the 2021-2027 multi-annual financial framework (C(2021)35).

or no prefinancing). The prefinancing will be paid 30 days from entry into force/10 days before starting date/financial guarantee (if required) – whichever is the latest.

There will be one or more **interim payments** (with cost reporting through the use of resources report).

Payment of the balance: At the end of the project, we will calculate your final grant amount. If the total of earlier payments is higher than the final grant amount, we will ask you (your coordinator) to pay back the difference (recovery).

All payments will be made to the coordinator.



Please be aware that payments will be automatically lowered if one of your consortium members has outstanding debts towards the EU (granting authority or other EU bodies). Such debts will be offset by us — in line with the conditions set out in the Grant Agreement (*see art 22*).

Please also note that you are responsible for keeping records on all the work done and the costs declared.

Prefinancing guarantees

If a prefinancing guarantee is required, it will be fixed in the Grant Agreement (*Data Sheet, point 4*). The amount will be set during grant preparation and it will normally be equal or lower than the prefinancing for your grant.

The guarantee should be in euro and issued by an approved bank/financial institution established in an EU Member State. If you are established in a non-EU country and would like to provide a guarantee from a bank/financial institution in your country, please contact us (this may be exceptionally accepted, if it offers equivalent security).

Amounts blocked in bank accounts will NOT be accepted as financial guarantees.

Prefinancing guarantees are formally NOT linked to individual consortium members, which means that you are free to organise how to provide the guarantee amount (*by one or several beneficiaries, for the overall amount or several guarantees for partial amounts, by the beneficiary concerned or by another beneficiary, etc*). It is however important that the requested amount is covered and that the guarantee(s) are sent to us in time to make the prefinancing (scanned copy via Portal AND original by post).

If agreed with us, the bank guarantee may be replaced by a guarantee from a third party.

The guarantee will be released at the end of the grant, in accordance with the conditions laid down in the Grant Agreement.

Certificates

Depending on the type of action, size of grant amount and type of beneficiaries, you may be requested to submit different certificates. The types, schedules and thresholds for each certificate are fixed in the Grant Agreement (*Data Sheet, point 4 and art 24*).

Liability regime for recoveries

The liability regime for recoveries will be fixed in the Grant Agreement (*Data Sheet point 4.4 and art 22*).

For beneficiaries, it is one of the following:

- limited joint and several liability with individual ceilings — *each beneficiary up to their maximum grant amount*
- unconditional joint and several liability — *each beneficiary up to the maximum grant amount for the action*

or

- individual financial responsibility — *each beneficiary only for their own debts.*

In addition, the granting authority may require joint and several liability of affiliated entities (with their beneficiary).

Provisions concerning the project implementation

Security rules: *see Model Grant Agreement (art 13 and Annex 5)*

Ethics rules: *see Model Grant Agreement (art 14 and Annex 5)*

IPR rules: *see Model Grant Agreement (art 16 and Annex 5):*

- background and list of background: Yes
- protection of results: Yes
- exploitation of results: Yes
- rights of use on results: Yes
- access to results for policy purposes: Yes
- access to results in case of a public emergency: Yes
- access rights to ensure continuity and interoperability obligations: Yes

Communication, dissemination and visibility of funding: *see Model Grant Agreement (art 17 and Annex 5):*

- communication and dissemination plan: Yes
- dissemination of results: Yes
- additional communication activities: Yes
- special logo: No

Specific rules for carrying out the action: *see Model Grant Agreement (art 18 and Annex 5):*

- specific rules for PAC Grants for Procurement: No
- specific rules for Grants for Financial Support: No
- specific rules for blending operations: No

Other specificities

n/a

Non-compliance and breach of contract

The Grant Agreement (chapter 5) provides for the measures we may take in case of breach of contract (and other non-compliance issues).

 For more information, see [AGA — Annotated Grant Agreement](#).

11. How to submit an application

All proposals must be submitted directly online via the Funding & Tenders Portal Electronic Submission System. Paper applications are NOT accepted.

Submission is a **2-step process**:

a) **create a user account and register your organisation**

To use the Submission System (the only way to apply), all participants need to [create an EU Login user account](#).

Once you have an EU Login account, you can [register your organisation](#) in the Participant Register. When your registration is finalised, you will receive a 9-digit participant identification code (PIC).

b) **submit the proposal**

Access the Electronic Submission System via the Topic page in the [Search Funding & Tenders](#) section (or, for calls sent by invitation to submit a proposal, through the link provided in the invitation letter).

Submit your proposal in 3 parts, as follows:

- Part A includes administrative information about the applicant organisations (future coordinator, beneficiaries, affiliated entities and associated partners) and the summarised budget for the proposal. Fill it in directly online
- Part B (description of the action) covers the technical content of the proposal. Download the mandatory word template from the Submission System, fill it in and upload it as a PDF file
- Annexes (see *section 5*). Upload them as PDF file (single or multiple depending on the slots). Excel upload is sometimes possible, depending on the file type.

The proposal must keep to the **page limits** (see *section 5*); excess pages will be disregarded.

Documents must be uploaded to the **right category** in the Submission System otherwise the proposal might be considered incomplete and thus inadmissible.

The proposal must be submitted **before the call deadline** (see *section 4*). After this deadline, the system is closed and proposals can no longer be submitted.

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the [IT Helpdesk webform](#), explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

Details on processes and procedures are described in the [Online Manual](#). The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

12. Help

As far as possible, ***please try to find the answers you need yourself***, in this and the other documentation (we have limited resources for handling direct enquiries):

- [Online Manual](#)
- FAQs on the Topic page (for call-specific questions in open calls; not applicable for actions by invitation)
- [Portal FAQ](#) (for general questions).

Please also consult the Topic page regularly, since we will use it to publish call updates. (For invitations, we will contact you directly in case of a call update).

Contact

For individual questions on the Portal Submission System, please contact the [IT Helpdesk](#).

Non-IT related questions please contact: [Here](#)

Please indicate clearly the reference of the call and topic to which your question relates (see cover page).

13. Important



IMPORTANT

- **Don't wait until the end** — Complete your application sufficiently in advance of the deadline to avoid any last minute **technical problems**. Problems due to last minute submissions (*e.g. congestion, etc*) will be entirely at your risk. Call deadlines can NOT be extended.
- **Consult** the Portal Topic page regularly. We will use it to publish updates and additional information on the call (call and topic updates).
- **Funding & Tenders Portal Electronic Exchange System** — By submitting the application, all participants **accept** to use the electronic exchange system in accordance with the [Portal Terms & Conditions](#).
- **Registration** — Before submitting the application, all beneficiaries, affiliated entities and associated partners must be registered in the [Participant Register](#). The participant identification code (PIC) (one per participant) is mandatory for the Application Form.
- **Consortium roles** — When setting up your consortium, you should think of organisations that help you reach objectives and solve problems.

The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting going beyond 30% of the total eligible costs must be justified in the application.

- **Coordinator** — In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
- **Affiliated entities** — Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any).
- **Associated partners** — Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.
- **Consortium agreement** — For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.

- **Balanced project budget** — Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully (*e.g. own contributions, income generated by the action, financial contributions from third parties, etc*). You may be requested to lower your estimated costs, if they are ineligible (including excessive).
- **No-profit rule (n/a for FPAs)** — Grants may NOT give a profit (i.e. surplus of revenues + EU grant over costs). This will be checked by us at the end of the project.
- **No double funding (n/a for FPAs)** — There is a strict prohibition of double funding from the EU budget (except under EU Synergies actions). Outside such Synergies actions, any given action may receive only ONE grant from the EU budget and cost items may under NO circumstances declared to two different EU actions.
- **Completed/ongoing projects** — Proposals for projects that have already been completed will be rejected; proposals for projects that have already started will be assessed on a case-by-case basis (in this case, no costs can be reimbursed for activities that took place before the project starting date/proposal submission).
- **Combination with EU operating grants (n/a for FPAs)** — Combination with EU operating grants is possible, if the project remains outside the operating grant work programme and you make sure that cost items are clearly separated in your accounting and NOT declared twice (see [AGA — Annotated Model Grant Agreement, art 6.2.E](#)).
- **Multiple proposals** — Applicants may submit more than one proposal for *different* projects under the same call (and be awarded a funding for them).

Organisations may participate in several proposals.

BUT: if there are several proposals for *very similar* projects, only one application will be accepted and evaluated; the applicants will be asked to withdraw one of them (or it will be rejected).

- **Resubmission** — Proposals may be changed and re-submitted until the deadline for submission.
- **Rejection** — By submitting the application, all applicants accept the call conditions set out in this this Call Document (and the documents it refers to). Proposals that do not comply with all the call conditions will be **rejected**. This applies also to applicants: All applicants need to fulfil the criteria; if any one of them doesn't, they must be replaced or the entire proposal will be rejected.
- **Cancellation** — There may be circumstances which may require the cancellation of the call. In this case, you will be informed via a call or topic update. Please note that cancellations are without entitlement to compensation.
- **Language** — You can submit your proposal in any official EU language (project abstract/summary should however always be in English). For reasons of efficiency, we strongly advise you to use English for the entire application. If you need the call documentation in another official EU language, please submit a request within 10 days after call publication (for the contact information, see *section 12*).

- **Transparency** — In accordance with Article 38 of the [EU Financial Regulation](#), information about EU grants awarded is published each year on the [Europa website](#).

This includes:

- beneficiary names
- beneficiary addresses
- the purpose for which the grant was awarded
- the maximum amount awarded.

The publication can exceptionally be waived (on reasoned and duly substantiated request), if there is a risk that the disclosure could jeopardise your rights and freedoms under the EU Charter of Fundamental Rights or harm your commercial interests.

- **Data protection** — The submission of a proposal under this call involves the collection, use and processing of personal data. This data will be processed in accordance with the applicable legal framework. It will be processed solely for the purpose of evaluating your proposal, subsequent management of your grant and, if needed, programme monitoring, evaluation and communication. Details are explained in the [Funding & Tenders Portal Privacy Statement](#).

Annex 1**Digital Europe types of action**

The Digital Europe Programme will use the following actions to implement grants:

Simple Grants

Description: The Simple Grants are a flexible type of action used by a large variety of topics and can cover most activities. The consortium will mostly use personnel costs to implement action tasks, activities with third parties (subcontracting, financial support, purchase) are possible but should be limited.

Funding rate: 50%

Payment model: Prefinancing – (x) interim payment(s) – final payment

SME Support Actions

Description: Type of action primarily consisting of activities directly aiming to support SMEs involved in building up and the deployment of the digital capacities. This type of action can also be used if SMEs need to be in the consortium and make investments to access the digital capacities.

Funding rate: 50% except for SMEs where a rate of 75% applies;

Payment model: Prefinancing – (x) interim payment(s) – final payment

Coordination and Support Actions (CSAs)

Description: Small type of action (a typical amount of 1-2 Mio) with the primary goal to support EU policies. Activities can include coordination between different actors for accompanying measures such as standardisation, dissemination, awareness-raising and communication, networking, coordination or support services, policy dialogues and mutual learning exercises and studies, including design studies for new infrastructure and may also include complementary activities of strategic planning, networking and coordination between programmes in different countries.

Funding rate: 100%

Payment model: Prefinancing – (x) interim payment(s) – final payment

Grants for Procurement

Description: Type of action for which the main goal of the action and thus the majority of the costs consist of buying goods or services and/or subcontracting tasks. Contrary to the PAC Grants for Procurement (*see below*) there are no specific procurement rules (i.e. usual rules for purchase apply), nor is there a limit to 'contracting authorities/entities'. Personnel costs should be limited in this type of action; they are in general used to manage the grant, coordination between the beneficiaries, preparation of the procurements.

Funding rate: 50%

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance the procurements) – payment of the balance

PAC Grants for Procurement

Description: Specific type of action for procurement in grant agreements by 'contracting authorities/entities' as defined in the EU Public Procurement Directives

(Directives 2014/24/EU , 2014/25/EU and 2009/81/EC) aiming at innovative digital goods and services (i.e. novel technologies on the way to commercialisation but not yet broadly available).

Funding rate: 50%

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance the procurements) – payment of the balance

Grants for Financial Support

Description: Type of action with a particular focus on cascading grants. The majority of the grant will be distributed via financial support to third parties with special provisions in the grant agreement, maximum amounts to third parties, multiple pre-financing and reporting obligations.

Annex 5 of the model grant agreements foresees specific rules for this type of action regarding conflict of interest, the principles of transparency, non-discrimination and sound financial management as well as the selection procedure and criteria.

In order to assure the co-financing obligation in the programme, the support to third parties should only cover 50% of third party costs.

Funding rate: 100% for the consortium, co-financing of 50% by the supported third party

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance sub-grants) – payment of the balance

Framework Partnerships (FPAs) and Specific Grants (SGAs)

FPAs

Description: An FPA establishes a long-term cooperation mechanism between the granting authority and the beneficiaries of grants. The FPA specifies the common objectives (action plan) and the procedure for awarding specific grants. The specific grants are awarded via identified beneficiary actions (with or without competition).

Funding rate: no funding for FPA

SGAs

Description: The SGAs are linked to an FPA and implement the action plan (or part of it). They are awarded via an invitation to submit a proposal (identified beneficiary action). The coordinator of the FPA has to be the coordinator of each SGA signed under the FPA and will always take the role of single contact point for the granting authority. All the other partners of the FPA can participate in any SGA. There is no limit to the amount of SGAs signed under one FPA.

Funding rate: 50%

Payment model: Prefinancing – (x) interim payment(s) – final payment

Lump Sum Grants

Description: Lump Sum Grants reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature). The granting authority defines a methodology for calculating the amount of the lump sum. There is an overall amount, i.e. the lump sum will cover the beneficiaries' direct and indirect eligible costs. The beneficiaries do not need to report

actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented only part of the lump sum will be paid.

Funding rate: 50%

Payment model: Prefinancing – second (third) prefinancing (as there is no cost reporting) – final payment

Annex 2**Eligibility restrictions under Articles 12(5) and (6) and 18(4) of the Digital Europe Regulation****Security restrictions Article 12(5) and (6)**

If indicated in the Digital Europe Work Programme, and if justified for security reasons, topics can exclude the participation of legal entities *established* in a third country or associated country, or established in the EU territory but *controlled* by a third country or third country legal entities (including associated countries)³⁸.

This restriction is applicable for SO1 (High Performance Computing), SO2 (Artificial Intelligence) and SO3 (Cybersecurity), but at different levels.

- In the case of SO3, the provision is implemented in the strictest way. When activated, only entities established in the EU and controlled from EU MS or EU legal entities will be able to participate — with no exceptions.
- In SO1 and SO2, entities controlled by third countries or third country legal entities may be able to participate if they comply with certain conditions set up in the Work Programme. To that end, additional rules will be imposed on those legal entities, which need to be followed if they want to participate.

The activation of this article will make a number of specific provisions in the Grant Agreement applicable, such as country restrictions for eligible costs, country restrictions for subcontracting, and special rules for implementation, exploitation of results and transfers and exclusive licensing of results.

Strategic autonomy restrictions Article 18(4)

If indicated in the Digital Europe Work Programme, calls can limit the participation to entities *established* in the EU, and/or entities established in third countries associated to the programme for EU strategic autonomy reasons³⁹.

The application of this article will make a number of specific provisions in the Grant Agreement applicable, such as country restrictions for eligible costs, country restrictions for subcontracting, and special rules for implementation, exploitation of results and transfers and exclusive licensing of results.

 For more information, see [Guidance on participation in DEP, HE, EDF and CEF-DIG restricted calls](#).

³⁸ See Article 12(5) and (6) of the Digital Europe Regulation 2021/694.

³⁹ See Article 18(4) of the Digital Europe Regulation 2021/694.