DC4EU project is Co-funded by the European Union's Digital Europe Programme
under Grant Agreement no. 101102611

9.1 COMMUNICATION, DISSEMINATION & VISIBILITY PLAN

Revision: v.0.7

Work package	WP9/MS 9.1
Task	D9.1
Due date	31/05/2023
Submission date	
Deliverable lead	University of Porto
Version	0.7
Authors	University of Porto
Reviewers	ECCA, 3CL

Abstract	This document is the Communication, Dissemination and Visibility Plan (CDV Plan) for the EU-funded project, Digital Credentials for Europe (DC4EU). It sets out the communication, dissemination tools and strategies, providing guidelines for all the project partners to realise the greatest potential impact for the project. The DC4EU CDV Plan aims to define the Communication and Dissemination goals and strategies, identify target audiences and stakeholders, define the key messages, identify and establish the communication processes, channels and tools, and specify the key performance indicators.
Keywords	Digital Credentials, Digital Identity Wallet, Large-Scale Pilots

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	12/05/2023	1st version of the deliverable for comments	University of Porto
V0.5	31/05/2023	2nd version of the deliverable for COO	University of Porto, ECCA, 3CL
V0.6	17/11/2023	3rd version of the deliverable for COO	University of Porto, ECCA, 3CL
V0.7	14/11/2024	4th version of the deliverable (revised as per the request from the mid-term review)	Ignacio Alamillo (Logalty) – provided Appendix D on Standards, with input from WP3, WP5, ECCA, U Porto

Project co-funded by the European Commission in the Digital Europe Programme		
Nature of the deliverable:		**R**
Dissemination Level		
PU	Public, fully open, e.g. web	
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to DC4EU project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

EXECUTIVE SUMMARY

The current document is the Communication, Dissemination and Visibility Plan (CDV Plan) for the project Digital Credentials for Europe (DC4EU), co-funded by the European Commission. It sets out the communication, dissemination tools and strategies, providing guidelines for all the project partners to realize the greatest potential impact for the project. The DC4EU CDV Plan aims to define the Communication and Dissemination goals and strategies, identify target groups and stakeholders, define the key messages, identify, and establish the communication processes, channels and tools, and specify the key performance indicators.

The CDV Plan will ensure that the Consortium takes a proactive role in maximizing the project's potential. To guarantee the effective dissemination of the findings and recommendations from the DC4EU project upon its completion, it will be essential to engage with the key target groups and disseminate information to them throughout the project timeline. Developed at the outset of the project, the document will provide guidance to the partners' dissemination activities, together with describing how Work Package 9 (WP9) will collaborate with and support the other work packages. Using a wide variety of communication and dissemination actions, it will identify opportunities and actions for each of the partners within their own countries as well as on a European-wide basis, for the distribution of the findings and recommendations from the project.

To facilitate a better understating of the communication and dissemination strategy, the CDV plan outlines all the actions that will be developed. It also sets out procedures and guidelines for all dissemination activities to be followed by the partners within the project. Aligned with the best practices established, this document will be continuously updated, along the project timeline according to the outputs, achieved goals and other indicators that could potentially have an impact on the DC4EU objectives.

PROJECT BACKGROUND

Europe faces unprecedented changes, in which digital transformation and the Green transition are fundamental elements for the future of Europe. The eIDAS trust framework is undoubtedly one of the pillars of the European Union, which has laid the foundations of identity and trust in the digital world. The revision of this framework extends its scope of competence beyond identity, encompassing the Electronic Attestations of Attributes (EAA). Establishing the technical measures, processes, and procedures for establishing trust frameworks in sectoral areas will be crucial to the construction of a digital Europe.

DC4EU involves 21 European Union (EU) Member States, plus Norway and Ukraine, that will partake in the Project playing different roles and with varying levels of involvement. The project will focus on identifying and applying all these aspects in the Education field, focusing on the issuance of educational credentials and professional qualifications, and in the Social Security field by engaging in the execution of the Portable Documents A1 (PDA1) and the European Health Insurance Card (EHIC).

The European Digital Identity Wallet (EUDIW) will be a key element of hybridization for cross-sectoral and cross-border use cases (Identity, Signature, educational credentials and Social Security). Beyond the development of the Large-Scale Pilots (LSPs) and the recommendations for issuing institutions, relying parties, Member States (MS) and citizens, DC4EU will contribute to a new paradigm to citizens in the field of education and social security. It will also be fully aligned to the conclusions of the State of the Union address (091620) and European Council Conclusions (100220) for identity and data, the European Declaration on Digital Rights and Principles for the Digital Decade and to once only principle (enabling the citizens' perspective).

The project's main objective is to support cross-border, large-scale piloting of the EUDIW in compliance with the EU Toolbox process by 82 organizations from 23 countries (21 EU MS + Norway and Ukraine). For this purpose, it will develop four use cases with work scheduled for 24 months and divided into 9 work packages. The project is supported with the involvement of 43 public organizations and 49 private entities, including relevant sectoral institutions, ministries, and digitalization agencies of the various countries, developing a comprehensive model and an ambitious dissemination plan, guaranteeing the relevance and impact expected.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AB	Advisory Board
CDV	Communication, Dissemination and Visibility Plan
COO	Coordinator
DC4EU	Digital Credentials for Europe
EAA	Electronic Attestations of Attributes
EC	European Commission
EHIC	European Health Insurance Card
EIDAS	electronic IDentification, Authentication and trust Services
EUDIW	European Digital Identity Wallet
EU	European Union
KPI	Key Performance Indicators
MS	Member States
LSP	Large Scale Pilots
PDA1	Portable Document A1
PMC	Project Management Coordinator
QEAA	Qualified Electronic Attestations of Attributes
SEO	Search Engine Optimization
SC	Strategic Committee
SS	Social Security
UC	Use Cases
WP	Work Packages

1. INTRODUCTION

The DC4EU project main objective is to test interoperability and scalability in the national domain and multiple cross-border contexts, to provide feedback to the EC and MSs for iterative updates through specific coordination work packages, project management processes and tasks. The process will allow for comprehensive wallet testing using QEAA, EAA and credentials, and their national and cross-border functionalities in a pre-production environment and corresponding UCs. The EUDIW will be a fundamental element of hybridization for cross-sectoral and cross-border use cases (identity, signature, educational credentials and social security). DC4EU will contribute to a new paradigm for citizens in the field of education and social security, which is fully aligned with the European Council requirements for identity and data. It will also adhere to the European Declaration on Digital Rights and Principles.

The general objective will be to fulfil the large-scale piloting of the EUDIW with the aim of achieving the highest impact possible. To this extent, the objective's achievement will be measured on the basis of number of wallet issuing countries involved, number of wallet users, involvement of education and social security domain-related institutions, wallet transactions fulfilled, qualified electronic signatures issued and number of countries that will interface with the wallet in pre-production systems. Aligned with the Project's main objectives and with the communication tasks, the structure of CDV Plan establishes a 24-month roadmap with guidelines that will determine the required actions by creating a community of practice and leveraging on the extensive networks available to the consortium team members. The plan will focus on the following four key actions:

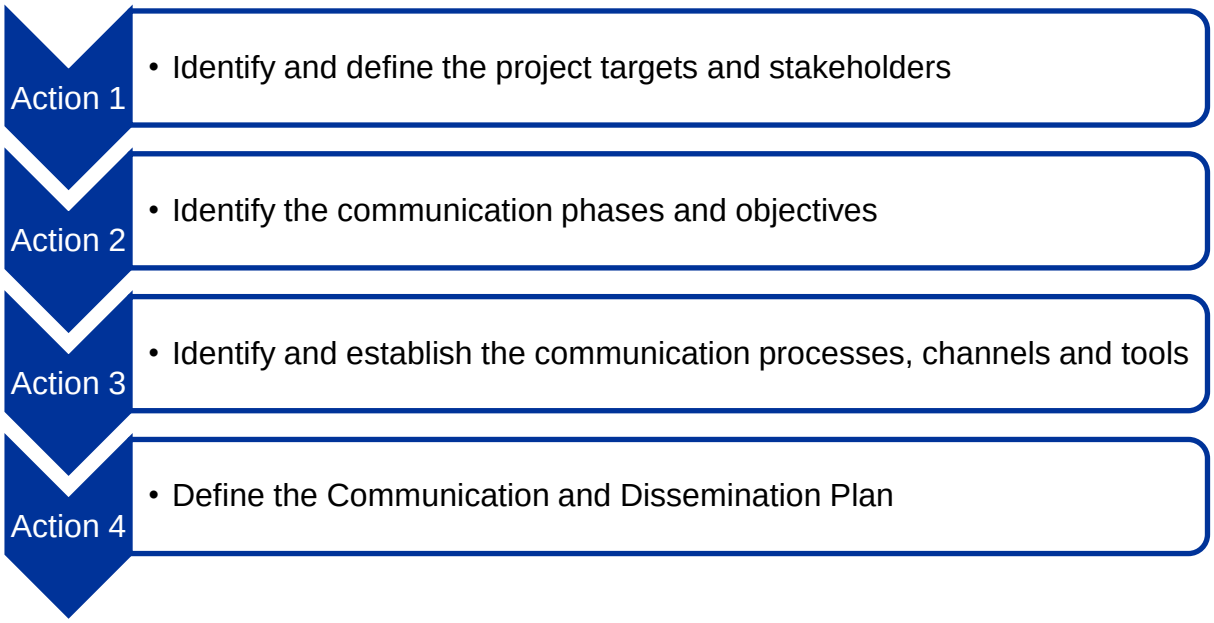

FIGURE 1 - CDV PLAN KEY-ACTIONS

These four key actions will result in a strategy to engage in a process of dialogue with all relevant stakeholders in a positive networking environment. It will harness experience and knowledge from experts, whilst also acquiring local understanding from the various conferences, workshops and events, that are described in this plan. The KPIs and metrics agreed upon will facilitate prominent awareness and exploitation of the project to realise its potential impact.

The project will enable the deployment of large-scale pilots that are necessary for the development, testing, validation (through iterative releases) and implementation of the new

EUDIW, a key component of the future eIDAS Regulation. The inclusion of public and private stakeholders in the consortium, an experienced multi-disciplinary Strategic Committee, and Advisory Board will contribute to a significant increase in the number of stakeholders in the eIDAS ecosystem. This will contribute to advancing the impact on meeting the objective of the Commission's Strategy on Shaping Europe's Digital Future.

The Consortium is focused on raising awareness, providing the necessary information about project results, engaging with partners, stakeholders and target groups in the process and directly involving them during the different phases of the project's development. In this sense, the current CDV Plan is provided to ensure that the Consortium will take a pro-active role in maximising the projects potential.

This WP9 ensures the project visibility, creates a community of practice, disseminates the findings and leverages on the extensive networks available to the consortium team members. It is also responsible for the identification of effective communication channels and tools between partners and the project coordinator, ensuring that all the information processes operate effectively and efficiently.

2. CDV PLAN STRUCTURE & PHASES

2.1. THE RATIONALE AND FUNCTION OF THE PLAN

Communication, dissemination and visibility are important requirements for the DC4EU project as it is essential to increase knowledge-sharing between the participating partners, together with enabling stakeholders to gain a good understanding of the project and its importance in scalability in a national domain and also in a multiple cross-border context. In order to maximize the spread of knowledge, there will be a strong focus of collaboration between the participants to avoid any boundaries between communication, dissemination, and visibility.

To maximize the project's impact, it is essential to communicate to society at large to demonstrate the project benefits to citizens. This CDV plan will be implemented to promote the development and deployment of use-cases for the new European Digital Identity ecosystem in pilot sites involving both public and private sector stakeholders, ensuring maximum visibility and awareness of the new European Digital Identity ecosystem.

The key attributes of the CDV plan include the following phases:

- Phase 1 - Information Collection and Awareness
- Phase 2 - Development of audience and target groups
- Phase 3 - Dissemination channels & tools implementation

Phase 1 will be focus on developing a unique strategy for information collection, which will incorporate a living document that will be updated throughout the life cycle of the project. It will also incorporate an instrument that will involve WP leaders contributing suitable information on their activities for dissemination. At each WP Leaders meetings, dissemination, communication, and visibility will be an agenda item and will involve input and updates from the WP leaders.

During this phase, the project will establish synergies with other similar initiatives, networks or organizations, particularly in the Member States, enforcing a common understanding for future potential collaborations. All partners in WP 9 are committed to working as a team to ensure that there is a consistent live process in place that is fully assessable to all participants in the project. In addition, is of upmost importance to ensure that information on each phase of the project's activities is available to the target audience at the earliest opportunity through the various dissemination channels and tools. The WP leaders will be responsible for ensuring the validation of content and material provided by their team. Phase 1 will go from Month 01 to Month 10.

Phase 2 will involve extensive engagement with the project partners to develop a dissemination list that includes the relevant audience and target groups. WP leaders and partners will be encouraged to provide relevant contacts for inclusion in the dissemination list. In addition, partners in each country will be required to develop a local dissemination list of target groups. Since the LSPs will have completed the preparation, phase and will be in their initial evaluation step, DC4EU will use these first initial outcomes to organize dedicated events and present them at fairs and events, to attract more interest.

This phase is also essential to inform all the identified stakeholders about the DC4EU objectives and to liaise with potential partners. In this phase, the CDV activities will help to raise the awareness of the DC4EU project across Europe, particularly in the Member States, enabling the dialogue between current and potential stakeholders. Considering the type of activities to be developed during this phase, it is of significant importance to collect relevant

feedback to ensure that the third and final phase, dedicated to the dissemination of results, will have the expected impact. Phase 2 will take place between Month 4 to Month 20.

Phase 3 is structured to provide a range of channels and tools to maximize the effectiveness of the dissemination process both on a European and Global level. It will be focused on the exploitation and transferability of the results for the Community, ensuring that those are available and delivered in the most effective way possible to maximize the projects impact. Thus, this phase aims at contributing to the adoption of the project results in order to ensure the project sustainability and full exploitation. The project will gather the attention of end-users and other potential stakeholders by leveraging the integration of the pilots. This third and last phase is scheduled between Month 18 and Month 24.

Specific objectives for each Phase are indicated further, in this document.

2.2. OPERATIONAL STRUCTURE OF CDV PLAN

This structure as illustrated in Figure 2 consists of all partners. The implementation of the CDV plan will be the responsibility of WP9 Partners. WP leaders will provide input to WP9 with informative material for dissemination through the various communication tools. This will be done in an agreed structure though a nominated WP leader. All project partners will contribute to the development of the contents to be used for communication purposes throughout the project's duration. WP9 will work closely with the Strategic Management Committee, the Advisory Board and the Coordinator throughout the project to ensure the objectives of the CDV plan are implemented accordingly.

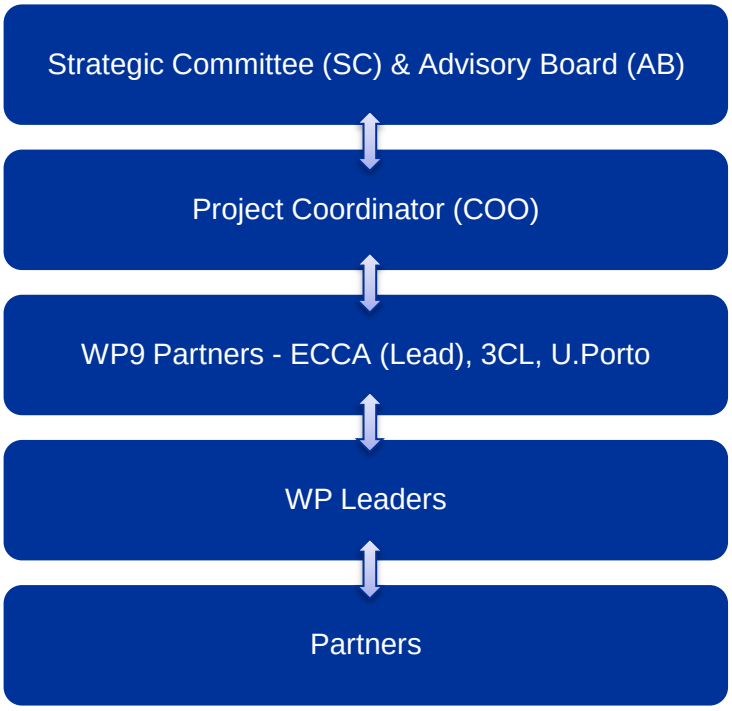

FIGURE 2 - CDV PLAN OPERATIONAL STRUCTURE

WP9 is implemented in close coordination with the PMC/COO and advised by the SC and AB. To that end, the consortium will carry out the following tasks in the communication domain:

CDV Plan

- Dissemination and communication tools and strategies, KPIs and metrics to facilitate the prominent visibility, awareness, and exploitation of the project, additionally providing guidelines for all the project partners to realise the greatest potential impact for the project on the business and scientific communities, as well as a plan to ensure the consortium will take a proactive role in maximising the projects' potential.

Dissemination Activities

- In coordination with the PMC/COO and all WPs, with the advice of the SC and AB, in order to maximise the impact of the project results in all domains. To this extent, the necessary subtasks will be foreseen to ensure the visibility of EU funding and that the project's dissemination is done in accordance with EU policy objectives, through the provision of a branding kit and guide, portal design, media and social media campaigns and events involving all relevant stakeholders.

Stakeholder management and standardization

- Developing a communication plan with relevant projects and stakeholders to avoid duplicities and promote synergies. Also, monitoring of ongoing work will be performed, case impacts on standardization bodies, and the creation of an engaged, expert community of practice.

FIGURE 3 - TASKS IN COMMUNICATION DOMAIN

2.3. CDV PLAN OBJECTIVES

Aligned with the previously described tasks in communication domain, the objectives of WP9 are to develop and implement a dissemination, communication, and visibility strategy in order to:

1. Promote the development and deployment of use-cases for the new European Digital Identity ecosystem in pilot sites involving both public and private sector stakeholders, which will include national agencies, public and private relying parties, attribute/credential/attestation providers, and wallet users (EU citizens and residents).

2. Ensure maximum visibility and awareness of the new European Digital Identity ecosystem, through widespread communication activities with existing stakeholders and a new wider audience, which is focused on improving citizen's access to highly trusted and secure electronic identity.

3. Develop programmes that enhance the promotion and awareness of the new European Digital Identity to align with standardisation and regulatory bodies.

4. Address social acceptability issues by carrying out target communication actions with policy makers and society.

FIGURE 4 – WP9 OBJECTIVES

To achieve these objectives, three main communication and dissemination phases were identified for the CDV Plan development:

2.3.1. PHASE 1 MAIN OBJECTIVES - INFORMATION COLLECTION AND AWARENESS

The Phase 1 will take place from Month 1 to Month 10 and the bellow mentioned main objectives were established.

Phase 1 - Month 1 - Month 10

- Identify target groups and stakeholders;
- Create a link between the Consortium and all the targets/stakeholders;
- Promote dialogue and synergies between the main stakeholders;
- Raise awareness on the project's concept and objectives;
- Encourage the interest in the DC4EU project main objective from the Community side;
- Enable the creation of a Community of Practice.

FIGURE 5 - CDV PLAN PHASE 1 MAIN OBJECTIVES

2.3.2. PHASE 2 MAIN OBJECTIVES - DEVELOPMENT OF AUDIENCE AND TARGET GROUPS

The Phase 2 will take place from Month 4 to Month 20 and the bellow mentioned main objectives were established.

Phase 2 - Month 4 - Month 20

- Engage the target groups to better identify their needs;
- Investigate and propose exploitation opportunities and business models for project results;
- Encourage the sustainability of the project's outcomes;
- Reinforce the Community of Practice foundations;
- Deploy activities aligned with the Sustainability and Transfer strategy;
- Liaise with stakeholders;
- Involvement of Member States public bodies so they can contribute to the dissemination in their respective countries and have influence in Pan-European communication network;
- Involve the standardisation sector.

FIGURE 6 - CDV PLAN PHASE 2 MAIN OBJECTIVES

2.3.3. PHASE 3 MAIN OBJECTIVES - DISSEMINATION CHANNELS & TOOLS IMPLEMENTATION

The Phase 3 will take place from Month 18 to Month 24 and the bellow mentioned main objectives were established.

Phase 3 - Month 18 - Month 24

- Disseminate project's outcomes, and guarantee the exploitation, replication and transferability of the results;
- Encourage the sustainability of the project's outcomes;
- Work to improve the social acceptability of the project's outcome by focusing on the increased levels of confidence and trust it will add.

FIGURE 7 - CDV PLAN PHASE 3 MAIN OBJECTIVES

2.3.4. TARGET GROUPS AND STAKEHOLDERS

Based on the target groups outlined, specific DC4EU stakeholders will be identified by the consortium.

Target groups and Stakeholders

- Higher Education Institutions and Alliances;
- Government and National agencies;
- Public and private sectors;
- Attribute/credential/attestation providers;
- Wallet users (EU citizens and residents).
- Technology companies;
- Policy makers / regulatory authorities;
- European Commission - should be kept updated with precise information on the project development, while developing synergies with other ongoing European initiatives that cover related topics (for example: other LSPs);
- Press and sectoral Media;
- Other relevant projects & digitalisation initiatives (e.g. LSPs).

FIGURE 8 - TARGET GROUPS AND STAKEHOLDERS

3. CDV CHANNELS/TOOLS & ACTIVITIES

3.1. CHANNELS AND TOOLS

Dissemination relates to the public communication of project outcomes. The entire DC4EU consortium is committed to approach and mobilize the appropriate stakeholders to multiply the effects of the project activities and maximize the impact.

After the definition of the communication phases and stakeholders, the analysis of potential channels and tools for the dissemination activities will take place. In this sense, the consortium shall take advantage of the existing internal channels and tools, as well of the ones belonging to partners or externals. For each channel and tool, a set of activities that can be applied to meet the CDV objectives along the three pre-defined communication phases.

To meet the requirements established for the three CDV Plan phases, the channels and tools below were identified. Offline tools, such as business cards and flyers were not considered since DC4EU focuses on the digitalisation processes.

3.1.1. DC4EU CHANNELS AND TOOLS

Online:

- Project Website Platform:

  The website, that can be accessed at https://dc4eu.eu, will serve as the main contact point for external users and as the main dissemination platform for the project. The website will be regularly updated with the new outcomes and results.

- Private Repository:

  The repository is used to store internal information for all the consortium members. All members can access the CDV contents dynamically, so the activities to be deployed can be facilitated.

- Digital Presentations:

  These will include common contents and messages. Standardized digital presentations for the project dissemination will be prepared for awareness sessions. This will facilitate the project dissemination.

- Social Media Platforms:

  The official DC4EU social media accounts on LinkedIn, Twitter and the YouTube platform will be used as strong means of communication and dissemination to achieve an almost unlimited number of users.

- Newsletter:

  The official DC4EU newsletter will be issued. The newsletter is another means of communication and has the potential to create relevant impact on the reader / user.

- Instant Messenger:

  Through the DC4EU account on Signal, for dynamic and secure communications inside (and to the outside of) the Consortium.

- Scientific Publications,

  To be prepared and published by members of the DC4EU Consortium.

- Standardization Contributions,

  Liaison with standardization bodies and working groups.
- Liaison with EU and International Projects:

  Including other LSPs, concretely EWC, NOBID and POTENTIAL
- Github/Gitlab:

  Managed by the technical WPs, where code and guidelines will be published.

Events:

- Engagement with Technical Workshops and Conferences:
- Key events and dissemination opportunities to be identified by the Consortium to increase the DC4EU visibility impact.

Press and media:

- Project Launch Press Release,

A number of press releases will be published in order to maximise the awareness and exposure of the project within and outside the consortium. These will be released at relevant times during the project and or relating to a particular event. Press releases shall contain information related to the activities developed internally, more precisely the ones that are related to the public outcomes. They should also include information related to the participation in dissemination events, such as Workshops, Webinars and Conferences.

3.1.2. DC4EU CONSORTIUM MEMBER CHANNELS AND TOOLS

Online:

- Digital promotional banners:

  To be published on the members' online channels and tools.
- Member Social Media:

  Engaging members' communities though their social media networks (LinkedIn and Twitter) and Youtube.
- Member Newsletters:

  Where content disseminated through DC4EU newsletters shall be included. As mentioned above, the newsletter is another means of communication and has the potential to create relevant impact on the reader / user.

3.1.3. DC4EU EXTERNAL CHANNELS AND TOOLS

Events:

- Engagement with Technical Workshops and Conferences:

  Key events and dissemination opportunities to be identified by the Consortium to increase the DC4EU visibility impact.

Press and media:

- Press Release:

  To be provided by DC4EU Consortium to the external.

3.2. CDV ACTIVITIES

Since DC4EU focuses on the digitalisation process, DC4EU will mainly use any digital media channel or communication framework to provide updated information to the relevant stakeholders. Nevertheless, presentations, brochures, and open-panel discussions will also play an important role raising awareness of the project.

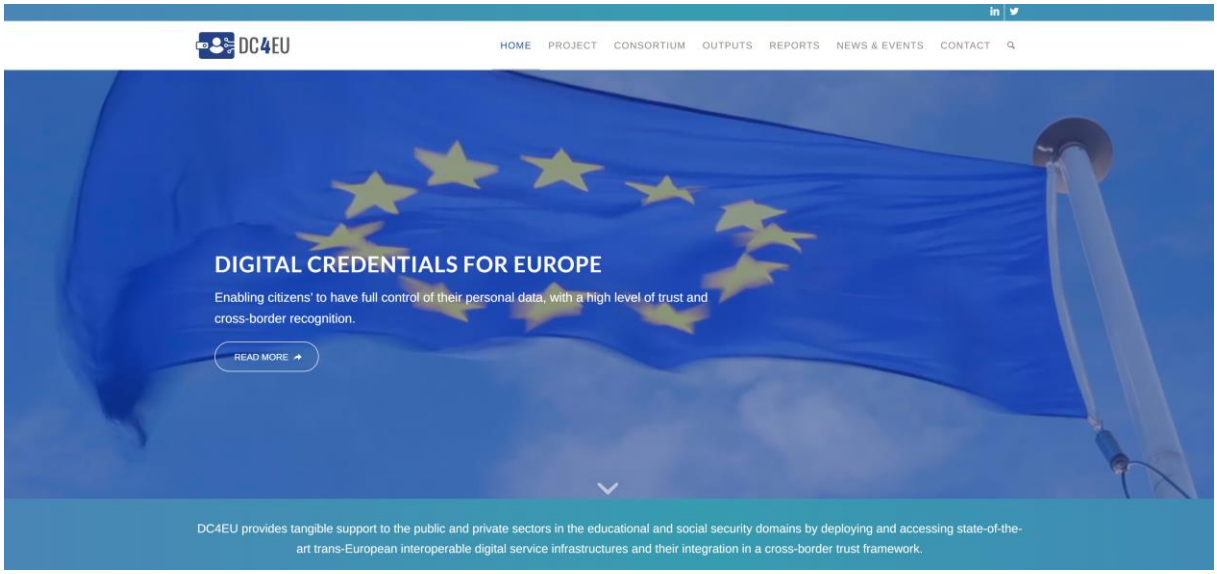

FIGURE 9 - DC4EU WEBSITE PLATFORM

The project website, available at https://dc4eu.eu, will serve as the major distribution tool. A project summary, objectives, consortium members, project deliverables will be available, together with the most recent news about the project and events. Periodical updates of the website will be carried out. Moreover, in order to assure good visibility of the project, the website has to be properly indexed by the most important and used search engines (i.e. Google, Bing, etc.). Therefore, SEO actions will be taken.

As the deliverables are the most direct and complete way of describing the activities of the project, DC4EU website will host all the project's public deliverables.

The initial months of the project's communication activities will be devoted those related with gathering initial awareness of the target audience. These actions include:

- Design of project branding: logo, project identity, information material, project templates.
- Design, development and publication of the project website.
- Set up a common private repository to store internal information for all the consortium members.
- Set up the social media accounts in the most common business social networks, as LinkedIn, Twitter and a Youtube channel.

Social Media Tools	URL
LinkedIn	https://www.linkedin.com/in/digital-credentials-for-europe-9a298025a
Twitter	https://twitter.com/DC4EU_project
YouTube	https://www.youtube.com/@DC4EUProject

TABLE 1 - SOCIAL MEDIA TOOLS URLS

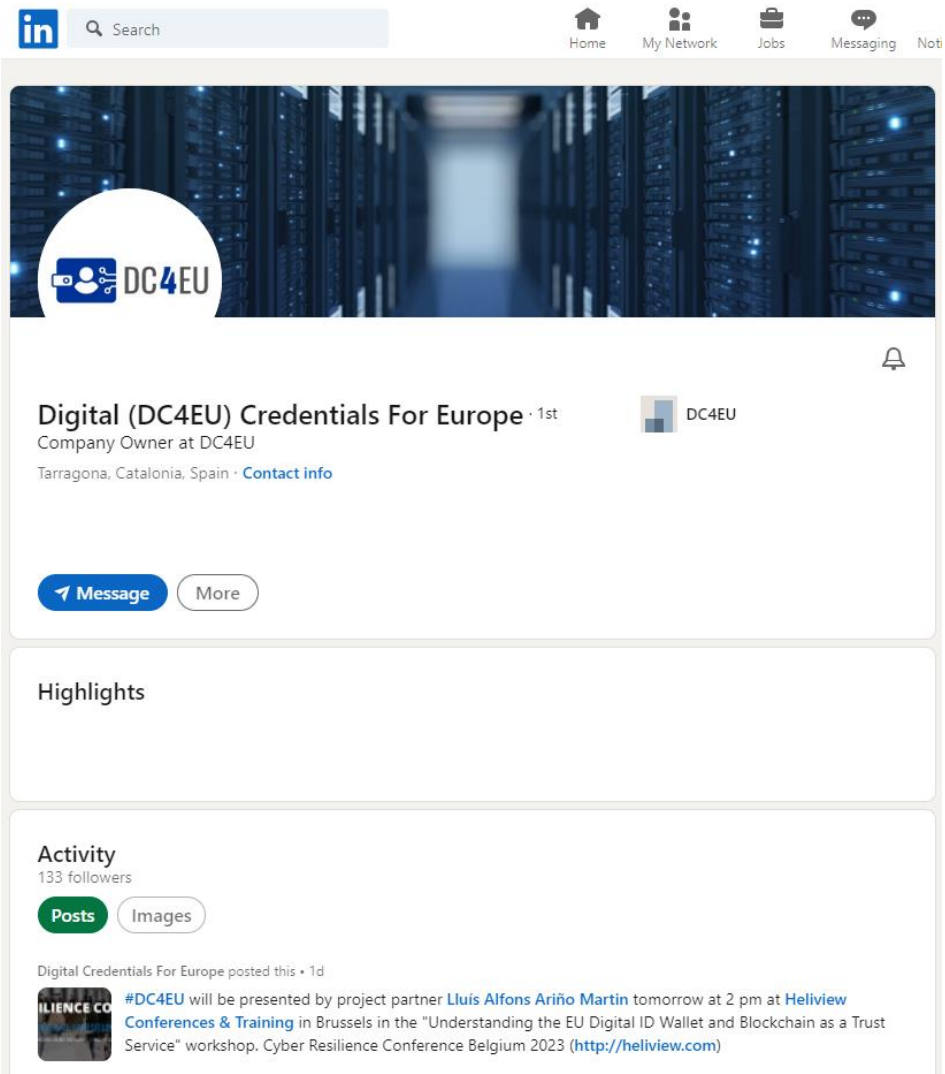

FIGURE 10 - DC4EU LINKEDIN PAGE

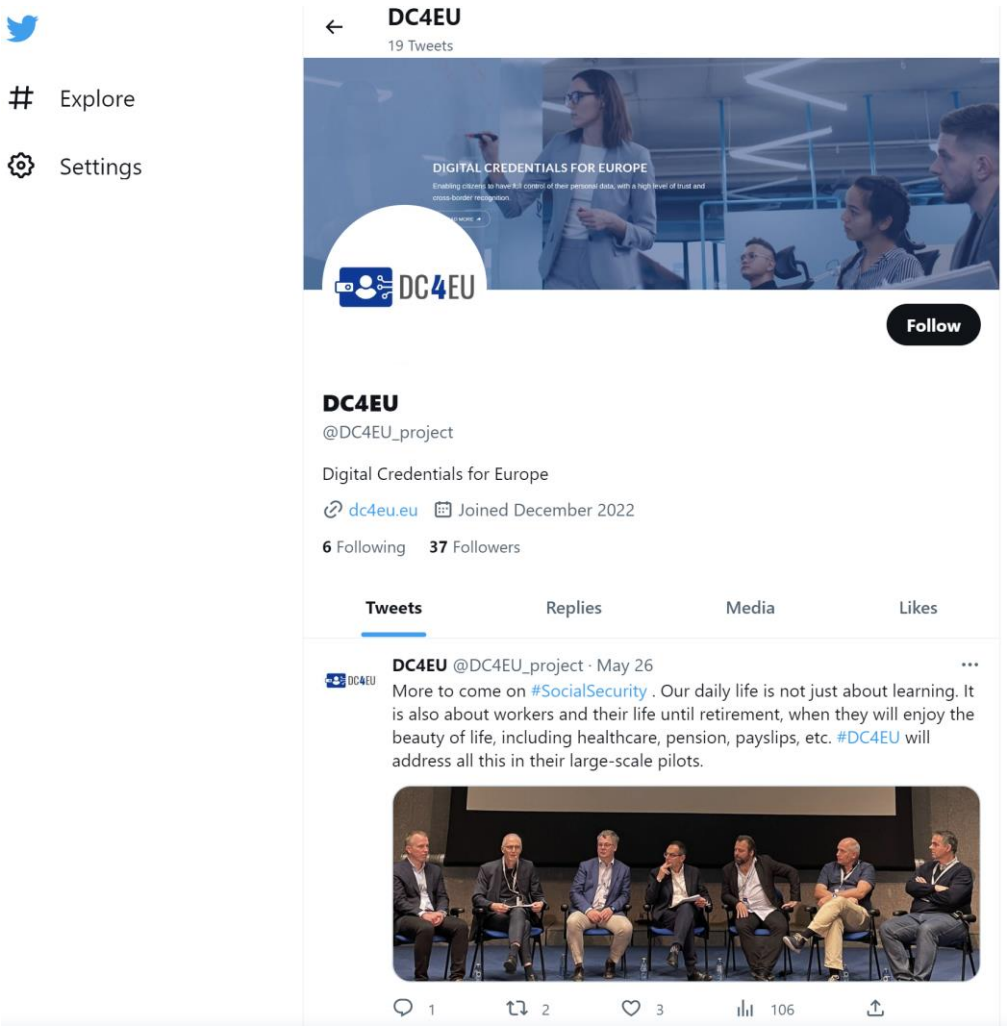

FIGURE 11 - DC4EU TWITTER PAGE

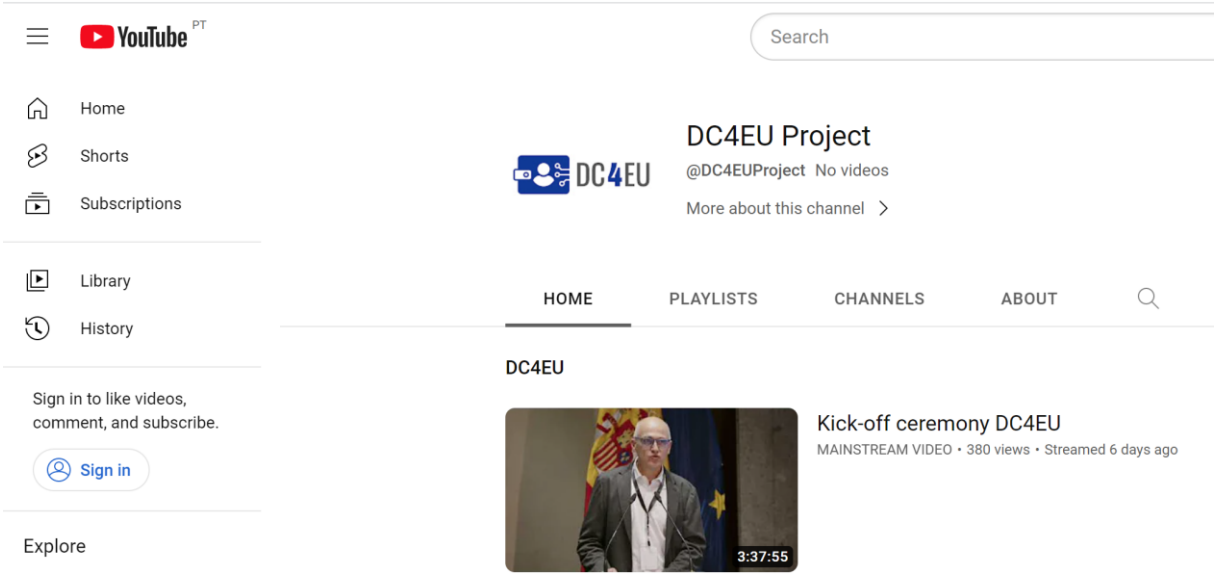

FIGURE 12 - DC4EU YOUTUBE CHANNEL

- Events, such as the Kick-Off meetings and the Final Conference will be critical for the

project success as they mark the beginning of the process and the end, where the sustainability strategy shall take place. Events-based dissemination are a critical part of the DC4EU strategy and activities. During the project lifespan all participations in events will be promoted through the DC4EU communication channels and tools, as well as through consortium members own channels. Liaison with stakeholders via dedicated events, such as conferences, webinars and workshops. These activities will contribute to utilising the research and innovation excellence of Europe and build a sustainable DC4EU network involving various stakeholders. To keep a record of such events, an online event excel sheet created by WP9 (Appendix B) will be available at the DC4EU private repository, where partners shall log their future events. After every event, the DC4EU partner(s) who joined the event will be requested to update the shared events list with all the relevant information and pictures to capture the experience, so that can be uploaded to social media, YouTube and website. To ensure that this process will flow, one person in each WP will be appointed as contact point for communication and dissemination materials (e.g. the WP leader).

- Liaison with other ongoing projects, related to Digital Credentials such as other LSPs, funded under the same scheme. The collaboration with these initiatives can potentially include co-organisation of events, information exchange related to project achievements and mutual social media promotion.
- Preparation of the Newsletter template and define the writing style to approach as wide an audience as possible.
- Set up a public open-source code repository to ensure not only easy collaboration on the development tasks between project partners, but also to gain project awareness beyond its frontiers.
- Carry out regular updates of the previously listed dissemination materials.

All these activities and their linked material will follow a unique a common visual identity. It is of the highest importance that the graphic image of the project is well defined at the very beginning of the project, and that all project members follow the guidelines on all materials and communications issued. In this sense, for instance, the project logo, which can be seen in Figure 13 was designed to express the project vision.

The project logo, which was developed at the commencement of the project will be essential for creating the project's identity and will be used on all dissemination materials. The composition of the DC4EU logo includes an artistic form of the project's acronym (DC4EU) and a digitised wallet with the symbol of a user. The wallet refers to a digital purse where users can store identity documents and social security details all in one place and allows users to reuse previously verified identities.

FIGURE 13 - DC4EU LOGO

The colour dark blue is used in the digital space with the meaning of trust, and in DC4EU, it also refers to the close alignment with the EU EU Digital Strategy, EU Data Strategy, Once Only principle, eIDAS Trust framework and GDPR. The colour white is associated with efficiency while giving a dynamic look and contrast to the dark blue colour.

The guidelines of the identity are composed of visual elements such as the fonts, colour palette and templates for documents and presentations. All dissemination materials refer to the project name and are in-line with the European Commission's guidelines.

A PowerPoint presentation template was created to be used by partners to create presentations for all external and internal events, meetings, etc. While the deliverable template presentation was created to be used by partners for submitting official reports, milestones and deliverables of the project.

The DC4EU project logo should be included in all dissemination materials, including the public and internal websites, brochures, flyers, presentations, roll-up, posters, both printed and online etc. Different quality logo versions are available.

Amongst the dissemination materials, a general PowerPoint presentation is provided. Each partner can add or modify information, or the context or event they are attending according to their needs. This generic presentation will initially include project objectives and a roadmap, contributing to create a recognizable project image. Throughout the project it will be updated to include the milestones the project will successfully achieve.

Additional DC4EU specific dissemination and communication actions involve events-based dissemination, where liaisons with relevant stakeholders or initiatives and projects researching on similar topics. The fruitful collaborations would result on the potential organization of joint events or the mutual media promotion. DC4EU will organize several events thought its lifetime, like the Kick-off meeting or the final conference as well as periodic webinars or workshops where the outcomes of the project will be depicted.

- Participation in exhibitions to initiate and maintain continuous interactions with stakeholders and to disseminate the project's results. Some examples of events include:
    - DC4EU Opening & Closing Ceremony
    - European Campus Card Association Annual Conference
    - EIC2023 Conference
    - EUNIS Conference
    - Cyber Resilience Conference
    - TNC23
- Publication of the results in scientific journals or conferences, and participation and organization of workshops and webinars both online and physical;
- Establish links with the open-source community and standardization bodies where DC4EU can promote the benefits of the solution designed and developed;
- Collaboration with other similar initiatives or projects to jointly contribute to the emergence of technical whitepapers, papers or even new standards;
- Establish regular communication with local and global authorities, citizens and user communities to promote the project and the need for trusted decentralized sharing of data.

In order to properly track the achievements in the dissemination, DC4EU partners will record the attendance and organization of events in the online event excel sheet created by WP9 (Appendix B). This same document will serve as a project wise agenda where any consortium member can include any relevant event DC4EU should participate in, allowing others to sign in, attend and disseminate the project.

3.3. CONTRIBUTION TO STANDARDS

Digital identity standards are essential for building a secure and interoperable digital society. By fostering collaboration, addressing emerging challenges, and aligning with regulatory frameworks, the standardisation community can ensure a future where digital identities are both secure and convenient. This will complement and become the basis for European or international standards, as they provide specific guidance for a particular country's digital identity landscape.

The European Standardisation Organisations (ESOs) will be pivotal in shaping the European digital identity landscape and developing standards for Trust Services, Personal Identification and Devices, Blockchain and Distributed Ledger Technologies. In addition, the international Standardisation Development Organisations (SDOs,) such as ISO, IEC and ITU, will help global collaboration on digital identity requirements to achieve interoperable standards that can be adopted worldwide. By collaborating through these SDOs, experts worldwide will contribute to creating global standards for secure and interoperable digital identity solutions.

The DC4EU project is actively involved and collaborating in several prominent SDOs, which include:

- ETSI TC ESI – Electronic Signatures and Infrastructures
- CEN TC 224 – Personal Identification, Electronic Signature, and Cards
- CEN/CLC/JTC 19 – Blockchain and Distributed Ledger Technologies
- ISO/TC 307 – Blockchain and Distributed Ledger Technologies
- ISO/IEC JTC 1/SC 17 – Cards and Personal Identification
- ISO/IEC JTC 1/SC 27 – Information Security, Cybersecurity, and Privacy Protection
- W3C – Decentralized Identifier Working Group & Verifiable Credentials Working Group
- Decentralized Identity Foundation
- FIDO Alliance – Identity Verification and Authentication Standards

In Appendix D, it outlines the on-going work of each SDO and the rationale of the work, together with explaining how the DC4EU project can contribute to using multiple standards.

As technology advances and societal needs evolve, digital identity standards are adapted to address emerging challenges and opportunities, such as the EUDI Wallet, Distributed Ledgers, Self-Sovereign Identities, Verifiable Credentials, Attestations of attributes and Online user identification. Along with these emerging challenges, there is also the need for alignment with regulatory frameworks, specifically eIDAS 2.0.

Collaboration among diverse players fosters a broader range of standards addressing various aspects of digital identity, facilitating tailored solutions to specific regions, and ensuring long-term compatibility and growth.

4. CDV IMPACT ASSESSMENT MONITORING

4.1. CDV KPIS

The necessary KPIs to measure and evaluate the success of the communication, dissemination and visibility activities throughout the duration of the project were defined and established. The Table 2 provides the KPIs that will enable the monitoring of the CDV Plan.

Communication, Dissemination and Visibility KPIs							
KPI #	**Channel / Tool**	**Impact**	**KPI**	**Target Group**	**KPI Goal 1**	**KPI Goal 2**	**KPI Goal 3**
4.1	Website at DC4EU.EU	Main information channel, communication of project results, news, events. Generate awareness on project	Page views	EC, Policymakers, Research Community, DC4EU Community of Practice	>10000	>15000	>25000
			Countries reached		>10	>25	>30
			Average stay time		>1min	>2min	>2min
4.2	Social Media Platforms	Brand building, increasing visibility to stakeholders active in social media, raising awareness of project and redirecting to news items on website when appropriate	# followers Twitter	Public, Community of Practice	>100	>350	>500
			# followers LinkedIn		>100	>100	>150
			# Social media posts		>100	>120	>200
			# Social media posts shared		>100	>200	>300
4.3	Instant Messenger	Facilitation of real-time and asynchronous communication	# of members on Signal	Members of DC4EU Working Groups, Community of Practice		>40	>100

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

4.4	Newsletters	Communication of project news, events, results to project subscribers	# of newsletters sent, views on web	DC4EU Community of Practice	1	4	8
			# of newsletters views on website		>100	>200	>500
4.5	Scientific Publications	Dissemination of knowledge and technologies developed	# papers published (conferences, journals)	Research Community		5	25
4.6	Standardization contributions	Contribution to the definition of new and existing standards	# of contributions	Community			2
4.7	Liaise with related EU & international Projects	Establish synergies, adapt to widely adopted references, exchange of information, create critical mass # of projects/initiatives liaised	# of projects/initiatives liaised with	Policy makers	0	5	10
4.8	Events: Technical Workshops (online)	Validation of approach, findings, dissemination of project activities. Engagement, awareness, involvement of industrial stakeholders and reach to pilot stakeholders	# international events attended	EC, Members of DC4EU Working Groups, Community of Practice		10	20
			# events organised to disseminate project results			3	8
			# attendees at final event/closing ceremony				>150
4.9	Github/Gitlab	Open-source availability of project software, media and artifacts	# contributions	Community		20	30
			# components			5	10

TABLE 2 - CDV KPIS

This above mentioned KPIs will be continuously tracked as indicators of the success of the dissemination and communication activities. For instance, the website activity (e.g. number of visitors, time spent, etc.) will be monitored through different tools like Google Analytics in order to gather information about the website traffic and how visitors interact. Same activities are planned for the social networks monitoring or the actual reach of the newsletters.

The analysis of the data gathered from all the dissemination will help us identifying potential barriers and risks that may prevent stakeholders from fully engaging with DC4EU. These could include legal, financial, or technical barriers, as well as cultural, social, or political issues that may impact their willingness to engage.

4.2. CDV INITIAL RISK ASSESSMENT

An important critical mission is to ensure that the strategy will remain on track. In order to avoid and/or mitigate potential risks, a risk management process will be implemented and will consist in a regular assessment of progress and risks towards progresses and the elaboration of a contingency plan to address the specific risks identified.

Every six months, the WP9 will check if the established KPIs for the previously project quarter were achieved. This process will allow the WP to define what potential measures could be applied to mitigate identified risks.

In the table below, we identify the potential risks related with this CDV implementation, as well as the potential impact and the consequential remedial actions to guarantee the established KPIs are achieved. The initial risk assessment is a minimalist approach and new risks will be identified every six months, when the KPIs assessment takes place.

Description of the potential risk	Impact	Probability of occurrence	Remedial actions
KPIs are not reached according to the plan	Potential risks related to the project visibility	Low	Review activities execution performance and related processes/KPIs, if needed.
Changes in WP9 key staff/personnel during the project (e.g. turnover)	This would imply that the teams would have to allocate other personnel (or subcontract) for the execution of the related activities, potentially increasing costs and activities timeline.	Medium	Allocation of other personnel with the necessary skills to accomplish the established objectives.

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

Subcontracting delays	Delay in hiring companies/people will impact activities timelines.	Medium	Timely, strict and careful management of the procurement processes.
Time deviation in other WPs	Failing to comply with the proposal in time for the technical implementations, which would delay the project	Low	The Milestones were set to produce as much information as possible about the deliverables and to boost the interoperability among partners. If this situation happens, a reschedule of the activities will guarantee that the CDV will keep adjusted to the project objectives.

TABLE 3 – CDV INITIAL RISK ASSESSMENT

CONCLUSIONS

The current DC4EU Communication, Dissemination & Visibility Plan is flexible in order to allow content changes and new methods to meet the consortium needs during the project implementation. It will be a fundamental tool for the project's success, providing guidance to all the partners on the dissemination objectives and achievements.

All the partners are invited to contribute to the plan enhancement during the project's timeframe, and to register all the participations in events, actions, or communications to the media, in close collaboration with WP9.

The execution of this plan will generate contributions for the sustainability strategy of the project, thereby fulfilling DC4EU consortium objectives.

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

REFERENCES

[1] https://www.dc4eu.eu/

APPENDIX A – DELIVERABLES

- D1.1 Project Management Handbook
- D1.3 Quality assurance and risk management plan
- D1.4 Periodic reports
- D1.5 Final report
- D3.1 DC4EU Collaboration & Cooperation Strategy and Activities Report
- D3.2 Coordination report with eIDAS Expert Group
- D4.1 Issuance and verification legal analysis
- D4.2 Onboarding process analysis
- D5.1 Business Blueprint
- D5.2 Deployment and Testing Scenarios Results Library (DTSRL)
- D5.3 Initiatives mapping, documentation, and final report on LSP
- D6.1 The Business Blueprint (BBP)
- D6.2 The Deployment, Testing and Piloting Scenarios Results Library (DTSRL)
- D6.3 The Initiatives mapping and alignment checklist
- D8.1 Registers of governing authorities, verifiable data / trust / attribute / schema registries, guidelines for ecosystem member enrolment
- D8.2 Ecosystem auditing, certification, and sustainability guidelines
- D9.1 Dissemination, communication and visibility plan
- D9.2 Dissemination final report

APPENDIX B – RECORD OF DISSEMINATION EVENTS

DC4EU - Record of Dissemination Activities

Event Name	Event Type	Location / Online	Event Link	Date of Event	Partner	Presenter	# Attendees	DC4EU Post

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

APPENDIX C – KPI REPORT TEMPLATE (MM/YY – MM/YY)

Communication, Dissemination and Visibility KPIs						
KPI #	**Channel / Tool**	**Impact**	**KPI**	**Target Group**	**Actual**	**KPI Goal *n***
4.1	Website at DC4EU.EU	Main information channel, communication of project results, news, events. Generate awareness on project	Page views	EC, Policymakers, Research Community, DC4EU Community of Practice		
			Countries reached			
			Average stay time			
4.2	Social Media Platforms	Brand building, increasing visibility to stakeholders active in social media, raising awareness of project and redirecting to news items on website when appropriate	# followers Twitter	Public, Community of Practice		
			# followers LinkedIn			
			# Social media posts			
			# Social media posts shared			
4.3	Instant Messenger	Facilitation of real-time and asynchronous communication	# of members on Signal	Members of DC4EU Working Groups, Community of Practice		
4.4	Newsletters	Communication of project news, events, results to project subscribers	# of newsletters sent, views on web	DC4EU Community of Practice		
			# of newsletters views on website			
4.5	Scientific Publications	Dissemination of knowledge and technologies developed	# papers published (conferences, journals)	Research Community		

4.6	Standardization contributions	Contribution to the definition of new and existing standards	# of contributions	Community		
4.7	Liaise with related EU & international Projects	Establish synergies, adapt to widely adopted references, exchange of information, create critical mass # of projects/initiatives liaised	# of projects/initiatives liaised with	Policy makers		
4.8	Events: Technical Workshops (online)	Validation of approach, findings, dissemination of project activities. Engagement, awareness, involvement of industrial stakeholders and reach to pilot stakeholders	# international events attended	EC, Members of DC4EU Working Groups, Community of Practice		
			# events organised to disseminate project results			
			# attendees at final event/closing ceremony			
4.9	Github/Gitlab	Open-source availability of project software, media and artifacts	# contributions	Community		
			# components			

APPENDIX D – CONTRIBUTION TO STANDARDS

SDO		**ETSI TC ESI – Electronic Signatures and Infrastructures**	**Rationale**	**Develops standards for e-signatures, digital seals, and timestamping essential for legal and secure transactions in digital wallets, ensuring eIDAS compliance.**		
Work item		RTS/ESI-0019431-1. Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev.		Specifies generally applicable policy and security requirements for Trust Service Providers (TSPs) operating a remote signature creation device (SCDev).		In case DC4EU pilots the creation of remote qualified signatures and, more probably, seals by QEEA or Pub-EEA providers.
		RTS/ESI-0019432. Electronic Signatures and trust Infrastructures (ESI); Protocols for remote digital signature creation.		Specifies the components semantics referring to other existing standards for protocols specifications, where possible, specifically to CSC API for JSON protocol and OASIS DSS-X for XML protocol.		In case DC4EU pilots the creation of remote qualified signatures and, more probably, seals by QEEA or Pub-EEA providers.
		RTS/ESI-0019461. Electronic Signatures and		Update TS 119 461 to align with requirements		DC4EU pilots can provide contributions regarding the

		Trust Infrastructures (ESI); Policy and security requirements for trust service components for identity proofing of trust service subjects.		from the EU Digital Identity Framework. The revision covers the following: 1. Update requirements and use cases to reflect revised identity proofing requirements in the revised eIDAS Regulation, notably in Article 24.1. 2. Update to include both identity proofing for issuing of (Qualified) Electronic Attestation of Attributes and use of such attribute attestations in identity proofing processes. 3. In co-ordination with CEN TC224, provide a standard that is suitable as basis for the identity proofing part of PID onboarding to the EUDI Wallet.		user onboarding processes. Specifically, in the case of Pub-EEA issuers, that are not formally subject to Article 24 of the amended eIDAS Regulation but must provide an equivalent level of reliability.
		DTS/ESI-0019462. Electronic Signatures and Trust Infrastructures (ESI); Wallet interfaces		This TS is to specify interfaces enabling interaction of wallet and trust services including signing. More		DC4EU pilots can provide relevant contributions, especially regarding the

		for trust services and signing.		specifically this WI shall specify: - A wallet interface to trust service providers for the purpose of issuing attribute attestations and certificates to the wallet; - A wallet interface to trust service providers when the trust service provider acts as relying party in providing its services; - An interface for creation of electronic signature where the signing device is managed by a trust service provider; - Support for use cases for the creation of electronic signatures and other trust services and possible requirements for interfaces.		EBSI and OpenID Federation protocols.
		DTS/ESI-0019471. Electronic Signatures and Trust Infrastructures (ESI); Policy and Security		This TS is to specify policy and security requirements of attribute attestation trust service		DC4EU pilots can provide contributions regarding policy and security requirements. Specifically, in

		requirements for Providers of Electronic Attestation of Attribute Services.		providers and the attribute attestation services they provide. More specifically this WI shall specify: - Policy and security requirements on attribute verification and generation of attestations by the trust service provider; - Policy and security requirements on attribute attestation status validation services; - Requirements for assessing the trustworthiness of the attribute attestation; and - Requirements on personal data processing.		the case of Pub-EEA issuers, that are not formally subject to Article 24 of the amended eIDAS Regulation but must provide an equivalent level of reliability.
		DTS/ESI-0019472-1. Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestations of Attributes; Part 1: General requirements.		This TS is to specify profiles for Attribute Attestations. More specifically this WI shall specify: - Semantics for the components of attribute		DC4EU pilots can provide significant contributions, especially regarding SD-JWT-VCDM, aligned with W3C VCDM 2.0.

				attestations. This will include, among others, information as listed in Annex V of eIDAS 2.0. - Binding of semantics to profiling one or more syntaxes including those required by the EUDI Wallet Architecture and Reference Framework. The standard will not limit the types of attributes carried in an Attribute Assertion. The standard will support selective disclosure of attributes.		
		DTS/ESI-0019472-2. Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestations of Attributes Part 2: Profiles for Relying party interface to EUDI Wallet.		This TS is to specify interface protocols to: - authenticate the relying party and its attributes to the EU Digital Identity Wallet - authenticate the EU Digital Identity Wallet to the relying party - present wallet held attributes as selected by the wallet holder		DC4EU pilots can provide relevant contributions, especially regarding relying parties' registration and access based on the EBSI and OpenID Federation protocols.

				This interface protocol will meet the requirements of the EUDI Wallet Architecture and Reference Framework.		
		DTS/ESI-0019475. Electronic Signatures and Trust Infrastructures (ESI); Relying party authorisations for access to EUDI Wallet.		This TS specifies Requirements for relying parties attributes used to authorise requests for data from Digital Identity Wallets. This includes: - additional policy and security requirements for the issuing of certificates (certificates for electronic signatures, electronic seals and website authentication), or the issuing of electronic attestations, including such attributes. - requirements on the schema(s) for such attributes.		DC4EU pilots can provide relevant contributions, especially regarding relying parties' use of attributes schemas based on the EBSI and OpenID Federation protocols.
		DTR/ESI-0019477. Electronic Signatures and Trust Infrastructures		To identify objective and standardisation requirements for		DC4EU could contribute if a pilot implements electronic

		(ESI); Standardisation Requirements for Electronic Attestation of Attributes with Signatures.		inclusion of Electronic Attestation of Attributes (EAA) with electronic signatures or seals under Regulation (EU) 2024/1183 Regulation 910/2014. Signing documents, especially in the organizational context, could take a new dimension facilitated by the new European Digital Identity Framework. As Electronic Attestation of Attributes are expected to become mainstream, having the possibility to include the validation of these attributes (or the EAA itself) in a signed document will have immense benefits.		signatures where the signer role is attested. E.g.
		DTS/ESI-0019602. Electronic Signatures and Trust Infrastructures (ESI); Trusted lists; Data model.		The work shall be defining a data model for trusted lists, from which XML trusted lists specified in ETSI TS 119 612 are a specific instance. The data model shall allow for		DC4EU pilots can provide relevant contributions, especially with respect to QEEA and Pub-EEA providers and AS management based on the EBSI and OpenID Federation protocols.

				instances of trusted lists in other formats, such as JSON, CBOR or ASN.1. The data model objects shall be specific enough that they allow their use in RTS 119 605 for the purpose of the process defined within that standard (RTS 119 605).		
		DTS/ESI-0019605. Electronic Signatures and Trust Infrastructures (ESI); Trusted lists; Procedures for using and interpreting trusted lists.		This TS specifies requirements for determining whether a signed trust service token (i.e. signed data object generated by a trust service) has been issued by a trust service of a specific type listed in a given trusted list or set of trusted lists, and whether a specific status or a set of specific statuses is applicable to that trust service for a given date and time.		DC4EU pilots can provide relevant contributions, especially with respect to QEEA and Pub-EEA providers and AS management based on the EBSI and OpenID Federation protocols.

SDO	**CEN TC 224 – Personal Identification, Electronic Signature, and Cards**	**Rationale**	**Addresses standards for secure authentication, biometric data, and electronic signatures, aligning well with European requirements and enhancing wallet interoperability.**		
Work item	prCEN/TS 18098. Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets.	Scope	The document shall cover all the possibilities for the on-boarding of user within European Digital Identity Wallets: online and offline mode (as described in the regulation), but also remote and face to face on- Boarding.	Potential contribution	DC4EU pilots can provide contributions regarding the user onboarding processes.
	NWIP Guidelines for the on boarding of user personal identification data within European Digital Identity Wallets where the User is a legal person.		The purpose of this proposal is to provide clear guidance for the on boarding of a user (natural or legal person) personal identification data within a wallet whose user is a legal person.		Low relevance from DC4EU perspective.

SDO	**CEN/CLC/JTC 19 – Blockchain and Distributed Ledger Technologies**	**Rationale**	**Covers standards for interoperability, security, and privacy on blockchain, which are increasingly relevant for digital wallets using decentralized identity. It is the European "mirror" of ISO/TC 307.**		
Work item	PWI – Policy and Security Requirements on Trust Services on Electronic Ledger.	Scope	The purpose of the TS is to define a CEN Technical Specification for Policy, Functional and Security Requirements on (qualified) trust services for Electronic Ledger acc. Section 11. eIDAS incl. : - Overview and relationship to other (qualified) trust services - Policies and Practices - TSP Management and Operations - Functional and Technical Requirements.	Potential contribution	DC4EU uses cases based on EBSI can contribute.

	PNWI - TS Functional and interoperability requirements on Decentralized Identifier (DID).		The purpose of the TS is to define a CEN Technical Specification for Functional and interoperability requirements on Decentralized Identifier DID including: - Overview and relationship to other identifier types - DID Methods with special focus on DID:EBSI - Protocols, Key Management - Functional and Technical Requirements - Requirements on interoperability The aim is to ensure interoperability of DID methods and to simplify the utilization of DID within the eIDAS 2 framework and to identify an initial set of DID Methods to standardize, with a focus on widely used methods across the different categories.		DC4EU uses cases based on EBSI can make relevant contributions.

SDO	**ISO/TC 307 – Blockchain and Distributed**	**Rationale**	**Covers standards for interoperability, security, and privacy on blockchain, which are increasingly relevant for digital wallets using decentralized identity.**

	Ledger Technologies				
Work item	ISO/AWI 24876 – Blockchain and distributed ledger technologies — Privacy protection when involving trust anchors in DLT-based identity management.	Scope	In the context of a distributed ledger technology (DLT)-based identity management system, this document identifies the various types of trust anchors and analyzes the personally identifiable information (PII) of a data subject, processed by trust anchors. It examines the complete cycle of PII processing by trust anchors within a DLT-based identity management system. Additionally, it outlines privacy considerations, detailing both technical and organizational controls to protect the PII of data subjects managed by trust anchors. Furthermore, the document provides examples of PII protection measures within a DLT-based identity management system.	Potential contribution	DC4EU uses cases based on EBSI can make relevant contributions.
	ISO/PWI 23042 – Reference architecture for DLT-based		This document defines a reference architecture for DLT-based decentralized identity systems. This includes:		DC4EU uses cases based on EBSI can make really relevant contributions.

	decentralized identity.		- The lifecycle management of digital identities and associated attributes and credentials in a decentralized identity system including migration of individual digital identities into another system. - The lifecycle management of the relevant actors and entities, including digital wallets, within a decentralized identity system. - The use of trust anchors through a decentralized identity system. - The entire lifecycle management of the decentralized identity system.		

SDO	**ISO/IEC JTC 1/SC 17 – Cards and Personal Identification**	**Rationale**	**Focuses on standards for identity cards and personal ID, relevant to digital wallet functionalities and digital identity.**		
Work item	ISO/IEC CD TS 23220-3 – Cards and security devices for personal identification —	Scope	This technical specification provides building blocks for mobile eID-System infrastructures and normalizes protocols, interfaces and services for mdoc apps by:	Potential contribution	

	Building blocks for identity management via mobile devices — Part 3: Protocols and services for issuing phase.		— specifying interfaces for data interchange for installing of software in installation phase as well as issuing and deriving of attributes and credentials in issuing phase; — specifying security and data protection mechanisms; — applying privacy-enhancing mechanisms; — specifying discoverability mechanisms. Mechanisms for updating or revoking of attributes and credentials or mdocs are out of scope of this document and are provided by SA specific protocols.		
	ISO/IEC CD TS 23220-4 – Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 4: Protocols		This document specifies building blocks for the implementation of the operational phase of mobile eID systems and any other mdoc. This document specifies the interface between the mdoc App and mdoc Reader and the interface between		

	and services for operational phase.		the mdoc Reader and the issuing authority infrastructure. More specifically, it defines transport protocols for various RF solutions and for over the Internet. And it defines the application layers, in particular the request-response protocols between an mdoc App and mdoc Reader and between an mdoc Reader and issuing authority. It further defines the security mechanism for Issuer authentication, mdoc authentication and credential holder verification. This document also enables parties other than the issuing authority to: – use a machine to obtain the mdoc data; – tie the mdoc to the mdoc holder; – authenticate the origin of the mdoc data; – verify the integrity of the mdoc data.		
	ISO/IEC CD TS 23220-5 – Cards		This standard provides definition of confidence levels and covers		

	and security devices for personal identification — Building blocks for identity management via mobile devices — Part 5: Trust models and confidence level assessment.		trust models. Furthermore, this standard provides information about the mobile eID-document about quality of the mobile eID-document data which may be subject to threats. This document leverages Levels of Assurance to provide a confidence level assessment methodology intended to facilitate the evaluation scheme and related certification process for mobile eID system. This document addresses the following topics: - Confidence levels definition which incorporates type and relevance of the issuer in a specific issuance data domain, reliability of the data collection process, reliability of the device on which the mobile eID-document is provisioned, and binding to the legitimate holder and related multi-factor authentication. - Trust models that can be leveraged by mobile eID-App, including the definition of generic sets of criteria applied for the scoring of confidence levels grounded on identity proofing, device-credential binding, data status, and holder authentication;		

			levels of confidence criteria are correlated to the threats on mobile eID data and their respective mitigation measures. - Examples of reference to certification and assessment programs that can land trust in the mobile eID-App data e.g. NIST digital identity guidelines (SP800-63), Common Criteria, and eIDAS.		
	ISO/IEC CD TS 23220-6 – Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 6: Mechanism for use of certification on trustworthiness of secure area.		This document specifies mechanism for use of certification on trustworthiness of secure area that is defined in ISO/IEC 23220-1. This document aims at enabling secure area providers to describe capabilities and confidence level of secure area for verification by eID issuers and/or mobile eID Attestation service providers. This document specifies: - List of elements describing capabilities and confidence level of a secure area; - Structure and management for use of a certificate – affixed or not to the secure area – containing		

			the elements aforementioned above.		
	ISO/IEC AWI 23220-7 – Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 7: Registration Authority Procedures for Mobile Document.		This document establishes an ISO/IEC Registration Authority (RA) that hosts a list of registered mdoc types and namespaces in a machine- and human-readable format. It establishes a Registration Management Group (RMG) with agreed on high-level review functions for mdoc types and namespaces registrations. This registration process serves as a centralized list for existing mdoc types and namespaces and also provides an opportunity for the Registration Management Group of experts to provide valuable feedback to the mDoc type and namespaces creators.		

SDO	**ISO/IEC JTC 1/SC 27 – Information Security, Cybersecurity, and Privacy Protection**	**Rationale**	**Concentrates on identity management, data protection, and secure processing, foundational for ensuring user trust in digital wallets.**

Work item	ISO/IEC PWI TS 27569 – Personal identifiable information (PII) processing record information structure.	Scope	This document specifies an interoperable, open, and extensible information structure for recording information relevant to the processing of Personally Identifiable Information (PII). This document further provides guidance on the use of this information to support the: - provision of a record of PII processing to another entity within or outside the organisation; - provision of a PII processing record to the PII Principal in the form of a 'Privacy Receipt'; - exchange of PII processing information i.e. information on how PII is processed between information systems; and, - management of the lifecycle of PII processing as based in the use of specific lawful basis.	Potential contribution	
	ISO/IEC WD 29115.2 – Information security, cybersecurity and privacy protection – Entity authentication		This document provides a framework for managing entity authentication assurance in a given context. In particular, it: - specifies four levels of entity authentication assurance;		

	assurance framework.		- specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance; - provides guidance for mapping other authentication assurance schemes to the four LoAs; - provides guidance for exchanging the results of authentication that are based on the four LoAs; and - provides guidance concerning controls that should be used to mitigate authentication threats.		
	ISO/IEC DIS 24760-1 – IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts.		This document defines terms for identity management, and specifies core concepts of identity and identity management and their relationships. It is applicable to any information system that processes identity information.		
	ISO/IEC FDIS 24760-2 – IT Security and Privacy — A framework for identity		This document: - provides guidelines for the implementation of systems for the management of identity information, and		

	management — Part 2: Reference architecture and requirements.		- specifies requirements for the implementation and operation of a framework for identity management. This document is applicable to any information system where information relating to identity is processed or stored.		
	ISO/IEC DIS 24760-3 – IT Security and Privacy — A framework for identity management — Part 3: Practice.		This part of ISO/IEC 24760 provides guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2. This part of ISO/IEC 24760 is applicable to an identity management system where identifiers or PII relating to entities are acquired, processed, stored, transferred or used for the purposes of identifying or authenticating entities and/or for the purpose of decision making using attributes of entities. Practices for identity management can also be addressed in other standards.		

	ISO/IEC WD 24760-4.4 – IT Security and Privacy — A framework for identity management — Part 4: Authenticators, Credentials and Authentication.		This document provides guidance on implementing authentication and the use of credentials therein, in particular it: - describes models for implementing user authentication with different operational aspects; - specifies formal descriptions of authentication methods; - specifies requirements for authenticators and credentials -- managing the lifecycle, -- use in a federated context.		

SDO	**W3C – Decentralized Identifier Working Group & Verifiable Credentials Working Group**	**Rationale**	**Focuses on standards for decentralized identifiers and verifiable credentials, crucial for digital wallet interoperability across identity systems.**		
Work item	Decentralized Identifiers (DIDs) v1.0	Scope	This document specifies the DID syntax, a common data model, core properties, serialized representations, DID operations, and an explanation of the process	Potential contribution	DC4EU pilots using EBSI can contribute to the maintenance of the specification.

			of resolving DIDs to the resources that they represent.		
	Verifiable Credentials Data Model v2.0.	Scope	This specification provides a mechanism for expressing these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable.	Potential contribution	DC4EU pilots can contribute to the progress of the current candidate recommendation.
	Verifiable Credential Data Integrity 1.0.		This specification describes mechanisms for ensuring the authenticity and integrity of verifiable credentials and similar types of constrained digital documents using cryptography, especially through the use of digital signatures and related mathematical proofs.		DC4EU pilots can contribute to the progress of the current candidate recommendation.
	Verifiable Credentials JSON Schema Specification.		This specification provides a mechanism to make use of a Credential Schema in Verifiable Credential, leveraging the existing Data Schemas concept.		DC4EU pilots can contribute to the progress of the current candidate recommendation.
	Securing Verifiable Credentials using JOSE and COSE.		This specification defines how to secure credentials and presentations conforming to the Verifiable Credential data model [VC-DATA-MODEL-2.0] with		DC4EU pilots can contribute to the progress of the current candidate recommendation.

			JSON Object Signing and Encryption (JOSE), Selective Disclosure for JWTs [SD-JWT], and CBOR Object Signing and Encryption (COSE) [RFC9052].		
	Bitstring Status List v1.0.		This specification describes a privacy-preserving, space-efficient, and high-performance mechanism for publishing status information such as suspension or revocation of Verifiable Credentials through use of bitstrings.		DC4EU pilots can contribute to the progress of the current candidate recommendation.

SDO	**Decentralized Identity Foundation**	**Rationale**	**Focuses on standards for decentralized identifiers and verifiable credentials, crucial for digital wallet interoperability across identity systems.**		
Work item	Universal Resolver.	Scope	The Universal Resolver resolves Decentralized Identifiers (DIDs) across many different DID methods, based on the W3C DID Core 1.0 and DID Resolution specifications.	Potential contribution	DC4EU pilots using EBSI can contribute.

	Well Known DID Configuration.		This document describes the data format of the resource and the resource location at which Internet domain controllers can publish their DID Configuration.		Interesting potential contribution from the perspective of using OpenID Federation and EBSI as trust anchor store.
	Credential Manifest.		The Credential Manifest is a common data format for describing the inputs a Subject must provide to an Issuer for subsequent evaluation and issuance of the credential(s) indicated in the Credential Manifest, i.e. for a Subject to become a Holder.		DC4EU pilots using EBSI can contribute.

SDO	**FIDO Alliance – Identity Verification and Authentication Standards**	**Rationale**	**Sets standards for secure, password-less authentication, a critical feature for digital wallet security and user access.**

Work item	Credential Exchange Specifications.	Scope	Defines a standard format for transferring all types of credentials in a credential manager including passwords, passkeys and more in a manner that is secure by default. There are two draft specifications: Credential Exchange Protocol and Credential Exchange Format.	Potential contribution	