

**VACANCY NOTICE FOR A POST OF SECONDED NATIONAL EXPERT**

DG – Directorate – Unit	CNECT – Digital Society, Trust and Cybersecurity – Unit H.4
Post number in sysper:	387297
Contact person:	Norbert SAGSTETTER
Provisional starting date:	2 quarter 2025
Initial duration:	2 years
Place of secondment:	<input type="checkbox"/> Brussels <input checked="" type="checkbox"/> Luxemburg <input type="checkbox"/> Other:
Type of secondment	<input type="radio"/> With allowances <input checked="" type="radio"/> Cost-free
This vacancy notice is open to: <input checked="" type="radio"/> EU Member States as well as <input type="checkbox"/> The following EFTA countries: <input type="checkbox"/> Iceland <input type="checkbox"/> Liechtenstein <input type="checkbox"/> Norway <input type="checkbox"/> Switzerland <input type="checkbox"/> The following third countries: <input type="checkbox"/> The following intergovernmental organisations: ... <input type="radio"/> EFTA-EEA In-Kind agreement (Iceland, Liechtenstein, Norway)	
Deadline for applications	<input checked="" type="radio"/> 2 months <input type="radio"/> 1 month Latest application date: 25-02-2025

Entity Presentation (We are)

Unit CNECT.H.4 "eGovernment and Trust" leads policy development for a file at the core of the Commission's political priorities: Implementing the regulatory environment and technical architecture for a European Digital Identity based on the eIDAS Regulation (EU 910/2014, 2024/1183). The mission of the unit includes coordinating and facilitating policy, legal and technical implementation of a European Digital Identity in close cooperation with by Member States and private sector actors. The tasks of the unit include

close coordination with public and private stakeholders across the EU and in third countries, international outreach and the work with a variety of actors within the Commission, other EU institutions, companies and administrations. Implementing the European Digital Identity Framework will support Member States reach the Digital Decade target that all EU citizens should have access to secure, privacy-enhancing digital identity that can be used throughout the Union by 2030.

The unit is part of Directorate CNECT.H "Digital Society, Trust and Cybersecurity" that is responsible for the EU's cybersecurity policy.

The tasks of the unit for 2025 include:

- Supporting the implementation of the new Framework Regulation for a European Digital Identity;
- Ensuring the smooth transition to the new framework including the establishment of a new governance system for the European Digital Identity Wallets, national eID schemes and the trust services framework;
- Finalising implementing legislation;
- Finalising the Technical Architecture and Reference Framework for the European Digital Identity Wallets ("Toolbox") under development in close cooperation with a Member States Expert Group;
- Supervising the implementation of large scale pilot projects in areas such as: ehealth, digital driving license, exchange of diplomas, etc., in cooperation with other DGs;
- Developing a certification scheme for the European Digital Identity Wallets;
- Managing international outreach and mutual recognition of digital identity and trust service frameworks with third countries (including candidate countries, the US, Canada, India, Japan and Singapore);
- Implementing the eIDAS Regulation (EU 910/2014, 2024/1183) for eID and trust services.

We lead on these files in close cooperation with other Commission services in DG CNECT, DG DIGIT, DG SANTE, DG GROW, DG JUST, DG TRADE and EU agencies, such as ENISA. We work closely with Member States and a wide variety of stakeholders in the public and private sector.

Further information on our activities are available at: European Digital Identity | European Commission (europa.eu) and <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

Job Presentation (We propose)

We are looking for a Policy officer who would provide direct support to the Chief Technology Officer of CNECT Unit H4 in driving the technical vision and implementation of the European Digital Identity Wallet ecosystem. This role includes contribution in planning, executing, and delivering complex technology projects while acting as a proxy for the CTO when needed. By bridging engineering teams and institutional stakeholders, the role ensures projects are delivered on time and within scope. Responsibilities include contributing to the management of technical resources, and the coordination of activities and tasks, while proactively identifying and mitigating risks throughout the Digital Identity Wallet initiative.

Jobholder Profile (We look for)

Key Responsibilities:

- **Project management:** Develop and oversee project plans, timelines, resource allocation, and overall project delivery.
- **Stakeholder Engagement:** Establish and maintain strong relationships with senior technical and policy stakeholders.
- **Team Support:** Support a multidisciplinary, multicultural team, promoting collaboration and productivity.
- **Cross-functional Coordination:** Guide cross-functional teams including engineers, designers, and analysts to align project goals.
- **Progress Tracking:** Continuously monitor project milestones, ensuring adherence to objectives and timelines.
- **Risk Management:** Identify, address, and mitigate potential risks and issues to prevent project delays.

Qualifications:

- **Technical Expertise:** Comprehensive knowledge of software development, cloud technologies, and system architecture, combined with demonstrated success in managing complex IT projects and practical experience in Agile/Scrum methodologies.
- **Specialization in Digital Identity:** Proficient in digital authentication, identification systems, and data protection standards, with familiarity with industry standards and specifications.
- **Communication & Leadership:** Excellent communication, organizational, and leadership skills with the ability to work synergistically and effectively within teams.

Preferred Skills:

- **Project Management Tools:** Proficiency in tools like Jira, Trello, or MS Project.
- **Technical Background:** Formal training or practical experience in IT or software development.

Eligibility criteria

The secondment will be governed by the **Commission Decision C(2008) 6866** of 12/11/2008 laying down rules on the secondment to the Commission of national experts and national experts in professional training (SNE Decision).

Under the terms of the SNE Decision, you need to comply with the following eligibility criteria at **the starting date** of the secondment:

- Professional experience: at least three years of professional experience in administrative, legal, scientific, technical, advisory or supervisory functions which are equivalent to those of function group AD.
- Seniority: having worked for at least one full year (12 months) with your current employer on a permanent or contract basis.
- Employer: must be a national, regional or local administration or an intergovernmental public organisation (IGO); exceptionally and following a specific derogation, the Commission may accept applications where your employer is a public sector body (e.g., an agency or regulatory institute), university or independent research institute.
- Linguistic skills: thorough knowledge of one of the EU languages and a satisfactory knowledge of another EU language to the extent necessary for the performance of the duties. If you come from a third country, you must produce evidence of a thorough knowledge of the EU language necessary for the performance of his duties.

Conditions of secondment

During the full duration of your secondment, you must remain employed and remunerated by your employer and covered by your (national) social security system.

You shall exercise your duties within the Commission under the conditions as set out by aforementioned SNE Decision and be subject to the rules on confidentiality, loyalty and absence of conflict of interest as defined therein.

In case the position is published with allowances, these can only be granted when you fulfil the conditions provided for in Article 17 of the SNE decision.

Staff posted in a European Union Delegation are required to have a security clearance (up to SECRET UE/EU SECRET level according to [Commission Decision \(EU, Euratom\) 2015/444 of 13 March 2015](#)). It is up to you to launch the vetting procedure before getting the secondment confirmation.

Submission of applications and selection procedure

If you are interested, please follow the instructions given by your employer on how to apply.

The European Commission **only accepts applications which have been submitted through the Permanent Representation / Diplomatic Mission to the EU of your country, the EFTA Secretariat or through the channel(s) it has specifically agreed to.**

Applications received directly from you or your employer will not be taken into consideration.

You should draft your CV in English, French or German using the **Europass CV format** ([Create your Europass CV | Europass](#)). It must mention your nationality.

Please do not add any other documents (such as copy of passport, copy of degrees or certificate of professional experience, etc.). If necessary, these will be requested at a later stage.

Processing of personal data

The Commission will ensure that candidates' personal data are processed as required by Regulation (EU) 2018/1725 of the European Parliament and of the Council ⁽¹⁾. This applies in particular to the confidentiality and security of such data. Before applying, please read the attached privacy statement.

⁽¹⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39)