Report on the outcomes of a Short-Term Scientific Mission[1]

Action number: CA20111

Grantee name: Muhammad Usama Sardar

Details of the STSM

Title: Formal Specification and Verification of Attestation in Confidential Computing

Start and end date: 10/09/2023 to 14/09/2023

Description of the work carried out during the STSM

Description of the activities carried out during the STSM. Any deviations from the initial working plan shall also be described in this section.

(max. 500 words)

- I had discussions with the host Dr. Lilia about:
  - Equivalence properties (such as observational equivalence)
  - Safety properties (such as deadlock)
  - Expressive power of the languages
- I had a follow-up discussion with Dr. Markulf Kohlweiss and his Ph.D. student Lorenzo Martinico at University of Edinburgh.
- Based on the discussions, we improved and refined the initial draft of WG3 deliverable D5's output 3: Applications: formal specification and verification of security protocols in emerging and challenging contexts (such as attestation in Confidential Computing).

Description of the STSM main achievements and planned follow-up activities

Description and assessment of whether the STSM achieved its planned goals and expected outcomes, including specific contribution to Action objective and deliverables, or

[1] This report is submitted by the grantee to the Action MC for approval and for claiming payment of the awarded grant. The Grant Awarding Coordinator coordinates the evaluation of this report on behalf of the Action MC and instructs the GH for payment of the Grant.

publications resulting from the STSM. Agreed plans for future follow-up collaborations shall also be described in this section.

(max. 500 words)

- We have achieved the main goal the visit, i.e., we had discussions on the remaining open issues in the WG3 deliverable D5's output 3.
- We have a plan to finalize the deliverable by the end of this month.
- We have a plan to collaborate to continue this research in the next phase and publish the results.