Dear challenger,

Welcome to the 2025 *Authenticated Anonymity Architecture Hack-a-thon.*

Please spend a few minutes reading this document to understand the nature and rewards of the challenge. Not only will you be contributing to a worthy research project that touches fundamental rights and ethical concerns about the use of today's Internet, you can also ***earn some money*** by doing so.

The Authenticated Anonymity Architecture (AAA)

The Authenticated Anonymity Architecture (AAA) is a novel approach for ensuring strong and robust anonymity to authenticated users, ***as long as*** they behave ethically and legally. If the AAA works as intended, there is no way for intruders, hackers and snooping Internet companies to associate anonymous activities to the real name of its owner, *unless* there are serious reasons to suspect that they have acted illegally. If they are seriously suspected of illegality then a formal, open and irrepudiable process to disclose the identity of the suspected criminal perpetrators can be used to disclose their identities so they can face justice. To safeguard the anonymity of ethical users (e.g., from the inappropriate investigations), the process cannot begin without consensus from a variety of multi-national authorities.
In brief, the idea is to allow public authorities that manage official identity data, such as IDs, electronic signatures, and other registries, typically called NIPs (National Identity Providers), to issue a code that can be used to create a second, anonymous identity. This second identity is also registered and recognized by the same authorities, but cannot be linked back to the real one. For example, Mr. Smith can create a second identity, “Mr. Batman,” that is fully valid, meaning that services such as chat platforms or banks can verify it as legitimate. To achieve this, three cryptographically linked codes are generated:

PID (Public Identity Data): a code stored by the NIP and associated with the user’s real public identity in their database.
SID (Secret Identity Data): a code stored on the Blockchain, created by combining secrets generated by multiple NIPs (the Union of NIPs, or UIP). It is encrypted with the user’s public key, so only the user can decrypt it, and only all NIPs together can recover its association with the PID. The decrypted SID is stored in the user’s local application.
SAC (Secret Authentication Code): a one-time code provided by a NIP after receiving the user’s SID. The SID–SAC association is stored on the Blockchain and can be easily verified.

The crucial security property of AAA is that the association between the **SID and the PID** remains protected and can only be recovered through proper cooperation among the NIPs.

For this hackathon, we have prepared an initial implementation that can generate all these codes and provide a realistic simulation of the AAA architecture, including:

- creating a public identity,
- creating a private (anonymous) identity, and

- securely linking the two.

The host machines are running 16 NIP servers behind a load balancer on port 8888, as well as a local blockchain node on port 8545. The public and anonymous identities have been generated directly within the environment in which you are operating.

Your Mission

We are asking you to test the robustness and strength of this implementation and to let us know of weaknesses, bugs and security concerns about our implementation, our model, and our approach.

We will provide a fully working implementation of our system in an already deployed form (with several preactivated public and anonymous users) and ask you to carry out an hostile attack to its inner workings. Specifically, we ask you to

Try to identify (=find the public identity of) one or more non-criminal anonymous users

The Challenge

Rewards for Success

We will provide a list of SID codes belonging to anonymous (non-criminal) users, along with a separate list of PID codes that correspond to real identities.
We will award three types of rewards.

A. €600 for identifying all the non-criminal users whose SIDs are listed in *anonymous-identities.txt*.
   In practice, you must determine which PID in *public-identities.txt* each of these SIDs is associated with, without using any brute-force attack.
   A winning submission must include the correct SID–PID associations together with a clear description of all the steps required to reproduce the identification.
   An additional €200 will be awarded to submissions that also provide a detailed and implementable solution to fix the security vulnerability that enabled the identification.

B. If you cannot identify all the non-criminal users, you can still earn €200 for each successfully identified user from *anonymous-identities.txt*, up to a maximum of €600.
   A further €200 in total will be awarded to submissions that also provide a detailed and implementable solution to fix the security vulnerability used for the identification.
   Each winning submission must include the public identity code of the identified user, together with a clear description of the steps required to reproduce the identification.
   Participants who submit the full list of identities (i.e., reward A) cannot also claim rewards in this category.

C. € 100 to suggest any security concern of the current implementation that will be evaluated as worthy and meaningful by the evaluation committee.

Please note that prizes will be awarded for each different working approach to the challenge. Yet, in case of multiple similar approaches all resulting in a correct solution, only the first submitted solution will be awarded. The evaluation committee is the final judge on the level of differences necessary in the proposed solution to trigger a new full reward.

Keep in mind that the real challenge is to discover a method that reveals the association itself. Therefore, it is not interesting knowing them and therefore no prizes will be awarded for associations found by chance or through brute-force techniques. What we are evaluating is not the specific codes you submit, but the method you develop to uncover the associations between them.

Also please note that the implementers are aware of at least one bug in the current implementation that allows competent hackers to carry out all of the attacks. Only the first challenger exploiting this bug for a working attack will be given a full reward.

Challenge Specifications

Each participant is assigned a dedicated virtual machine (VM) on our computing infrastructure. Each VM runs a complete instance of the Authenticated Anonymity Architecture (AAA), including multiple Network Identity Providers (NIPs) with their databases containing the codes associated with mockup government-issued official identifiers, a local blockchain node (Hardhat), and the full AAA stack (Go backend, Node.js services, PostgreSQL, Docker Compose).

Participants have access to the AAA application that runs internally on the local browser, which generates cryptographic keys, interacts with the NIPs and the blockchain to request or retrieve PAC and SAC codes, and stores data in it.

The challenge evaluates participants' ability to analyze, exploit, and defend the AAA system while understanding the ethical and technical implications of identity deanonymization.

You will have 2 days from beginning to end to complete the challenge (Mon 24 November h. 23:59 AST or Tue 25 November h. 5:00 CET until Wed 26 November 2025 23:59 AST or Thu 27 November 2025 05:59 CET). The jury will process your solutions in the order of submission.

Narrative Context

A malware was able to copy from the local application of many users the code (SID) that is essential and unique for associating a public identity with the one-time code that an anonymous user can generate and use to connect to public services. Therefore, the correlation between anonymous and public identities has been exposed.
Knowing the real identity of an anonymous user can lead to significant harm to the person involved, such as blackmail.

Your task is to investigate the environment, identify vulnerabilities, and propose actions that reveal this association, which should be protected by a cryptographic mechanism.

Access Model

Many VMs replicating this structure run on university servers, and participants connect remotely to their assigned VM. They do not run the stack locally (although they could by downloading the code from GitHub).

Smart contracts deployed in the environment are immutable: participants may not alter the contract code, but they may modify the client-side components and the way they interact with the contracts (such as transactions, inputs, timing, etc.).

Each team is provided with a non-privileged user account on its VM to read the documentation, download the files with the codes, inspect logs, read local databases, and eventually modify application-level components.

- Root/sudo access is reserved for the hack-a-thon's administrators.
- All participant actions are logged and monitored; any attempt to access other teams' VMs or the infrastructure will result in immediate disqualification from the

hack-a-thon.

Task

As indicated previously, the task is to identify all (A) or one (B) of the public identities (PIDs) associated with one or more of the secret identities (SIDs) in the file *anonymous-accounts.txt*, using only the data and tools available within your assigned VM.

Participants may:

- Inspect source code, configuration files and the public repository https://github.com/UniBO-PRISMLab/AAA-Authenticated-Anonymity-Architecture.
- Analyze blockchain events and transactions on the local blockchain node.
- Observe client-side operations and API calls through the AAA web application.

In the repository you will also find a link to the paper that inspired the AAA architecture. The algorithms and the entire protocol flow are described step by step in that paper.

Rules and Limitations

- Work only within your assigned VM; cross-VM access is strictly prohibited.
- Smart contracts cannot be modified or redeployed.
- Outbound internet access is allowed for Docker pulls, package installation, and Let's Encrypt certificates only.
- Do not perform denial-of-service attacks or destructive actions. Brute force algorithms are not considered a valid approach to the attack.
- Actions outside the allowed scope will result in disqualification.

Deliverables

Submit to aaa@lists.cs.unibo.it (and f.vitali@gmail.com in CC) a single .pdf file containing:

- The name of the team, the identity of all team members, with contact details, email, physical location;
- A short report (max two pages) including the identified private identity codes (PIDs), the exact steps, tools, and reasoning used, and optionally (for additional reward) clear and implementable steps to close the security hole;
- Any supporting scripts or logs in an artifacts/ directory;
- A step-by-step reproduction instructions.

Subject of submission:
Submission by *[team name]* to AAA Hackathon November 2025

Ethics Note

The AAA Hackathon is an educational exercise on the intersection of privacy, authentication, and accountability. All data and identities are synthetic and randomly generated. Participants must operate ethically and within their assigned environments. Any attempt to exploit, damage, or access systems beyond the provided scope will result in immediate disqualification.