



Reproducible Builds for the eIDAS 2.0 Wallet

Advisor: **A-SIT Plus GmbH**




Motivation

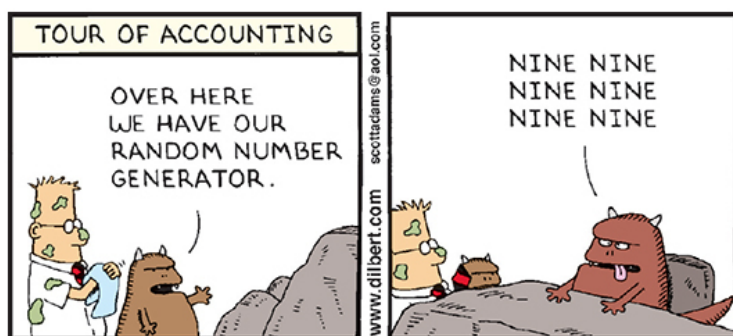
Open Source Software (OSS) is great – it allows anyone to check what the code is doing, and prevents any unexpected “features” from being snuck in. But: only few people truly build their software from source – and on some platforms, especially mobile platforms, it might not even be possible to do so.

So, many users will download pre-built binaries and execute them. How can we tell those pre-built binaries actually match the published source? Ideally, we could just build them from the published source, right? Well, it’s not that simple... build processes introduce lots of “randomness” in the form of timestamps, signatures, and more.

In this project, you will research the state-of-the-art in “reproducible builds”, and apply it to the build chain for complex real-world projects, such as the eIDAS 2.0 Wallet prototype.

Goals and Tasks

-  Research the state of the art
-  Try to apply it to real-world projects
-  Solve the problems you inevitably run into



It’s a feature, not a bug.

Literature

- > [M. Fourné et al.](#)
It’s like flossing your teeth: On the importance and challenges of reproducible builds for software supply chain security
[2023 IEEE Symposium on Security and Privacy \(SP\)](#)

Courses & Deliverables

- Master Project**
Project code
Report
Presentation

Recommended if you’re studying

- CS
- ICE
- SEM

Prerequisites

- > Interest in Open Source Software
- > Knowledge of build systems (Gradle)

Advisor Contact

research@a-sit.at