



# Lightweight Trust Verification on Constrained Devices by introducing a Trusted Third Party

Advisor: **Stefan More**





## Motivation

Electronic credentials can be used to authorize a person to access a resource. The entity verifying the credentials uses a policy to decide if the credentials provided by the user are trustworthy, and thus if access should be granted. This entity can not only be a person or website, but also a device.

Sometimes the device executing such a policy has limited computational resources – think about an access gate or car sharing. Additionally, it is not always possible to connect to the Internet during verification.

## Goals and Tasks

In this project we look into one strategy to free the verifying device from the heavy task of executing a policy. We introduce a **(trusted) 3rd party** which performs the checks and issues a lightweight confirmation to the user.

-  Understand SSI concepts and the concept of a policy language
-  Think about how to offload computation to a 3rd party
-  Implement prototype of idea
-  Perform benchmarks and compare approaches

## Literature

- > [G. Noble et al.](#)  
*Verifiable Credentials Data Model 1.0 W3C Recommendation*  
<https://www.w3.org/TR/vc-data-model>
- > [A. Abraham et al.](#)  
*Revocable and Offline-Verifiable Self-Sovereign Identities*  
*Trustcom 2020*

## Courses & Deliverables

- Introduction to Scientific Working**  
Short report on background  
Short presentation
- Bachelor Project**  
Project code and documentation
- Bachelor's Thesis**  
Project code  
Thesis  
Final presentation

## Recommended if you're studying

- CS
- ICE
- SEM

## Prerequisites

- > Java programming
- > Basic understanding of blockchains/distributed ledgers is beneficial

## Advisor / Contact

[stefan.more@iaik.tugraz.at](mailto:stefan.more@iaik.tugraz.at)