# Project: Concept for a Web-of-Trust-based certificate management in RIOT OS

|  |  |
| --- | --- |
| **Students** | Adarsh Raghoothaman,225874,adarsh.raghoothaman@st.ovgu.de |
|  |  |
| **Supervisor** | Frank Engelhardt |
| **Project start** | 01.04.2022 |
| **Project end** | 30.09.2022 |
|  |  |

# Project Goal

Digital certificates enables encryption and authentication when two devices communicate over the network. Most IoT platforms are cloud dependent and devices must be registered and managed via cloud interface. Cloud interface also provides certificates for devices in the network. This central management of certificates can be a single point of failure.

To avoid the problem the problem of single point of failure, decentralized solutions solutions based on Web of Trust(WoT) can be used. But the communication protocols and key management for this solution does not yet exit.

Thesis should propose a concept for certificate chain discovery and the implementation should run on RIOT operating system

# Projekt Plan

## Work Packages:

|  |  |  |  |
| --- | --- | --- | --- |
| **WP** | **WP Description** | **Work [Weeks]** | **Work**  **[%]** |
| 1 | Learning and research | 4,4 | 20% |
| 2 | Concept and programming | 11 | 50% |
| 3 | Evaluation and comparison | 2,2 | 10% |
| 4 | Text writing, slides, and presentation | 4,4 | 20% |
| Total: | | 22 | 100% |

## Time Plan:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **State** | **WP** | **Goal** | **Part Result / Material** | **Deadline** |
| Work | 1 | Literature review | Text | 28.04.22 |
|  | 2 | Specification of for certificate chain discovery | Text | 12.05.22 |
|  | 2 | Implementation | Code | 26.05.22 |
|  | 2 | Protocol refinement,resolve issues | Text,Code | 09.06.22 |
|  | 2 | Implementation | Code | 23.06.22 |
|  | 2 | Protocol refinement,resolve issues | Text,Code | 30.06.22 |
|  | 2 | Final Implementation | Code | 14.07.22 |
|  | 3 | Evaluation of solution in terms of communication overhead,Comparing with PKI | Text | 04.08.22 |
|  | 4 | Completing Report and Slides | Text, Slide | 08.09.22 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

State ∈{Work, Finished, Skipped}

Part Result / Material ∈ {Code, Text, Slide, Talk}